(19)日本国特許庁（ＪＰ）　(12) 公表特許公報（Ａ）　(11)特許出願公表番号

特表平10－505175

(43)公表日　平成10年(1998) 5月19日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６０

審査請求　未請求　予備審査請求　有　（全 76 頁）

(21)出願番号　特願平8－508954
(86)（22)出願日　平成７年(1995) ８月29日
(85)翻訳文提出日　平成９年(1997) ２月28日
(86)国際出願番号　ＰＣＴ／ＵＳ９５／１１０１６
(87)国際公開番号　ＷＯ９６／０７１５６
(87)国際公開日　平成８年(1996) ３月７日
(31)優先権主張番号　０８／２９８，９９１
(32)優先日　1994年８月31日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　ペリフェラル　ビジョン　リミティド
イギリス国，サマセット　ピーエー11　3イージー，フロム，パリス　ロード　57，パリス　ハウス
(72)発明者　スミシーズ，クリストファー　ポール　ケネス
イギリス国，ウインボーン　ピーエイチ21　3ディーダブリュ，コルフェ　ミュレン，パイン　ロード　18
(74)代理人　弁理士　石田　敬　（外３名）

最終頁に続く

(54)【発明の名称】　手書き署名を採取し、記憶し、伝送し、および、認証する方法ならびにそのシステム

(57)【要約】
手書き署名を採取し確認するためのコンピュータベースの方法およびシステム。手書き署名は、電子的に記憶された文書といったような文書に関連する可能性がある。文書の画像が表示され、手書き署名が採取される（４）。手書き署名に関係する一揃いの計測値が決定され、署名エンベロープ（10）の中に記憶される。任意には、文書の検査合計値を決定し署名エンベロープ内に記憶することができる。署名者の請求されたアイデンティティも同様に署名エンベロープ内に記憶できる。署名エンベロープはコード化される（104）。署名エンベロープをもう１つのアプリケーションまたはコンピュータ・プラットフォーム（26）に通信することもできるし、または後に確認を行なうために記憶することもできる。署名エンベロープは復号され、署名エンベロープ内に記憶された一揃いの計測値は、署名者（６）のアイデンティティを確認するべく手書き署名測定値の既知のセットに対して比較される。システムには、確認済み署名情報（12）を記憶する署名テンプレートのデータベースが含まれている。確認済みの一揃いの署名計測値は、類似性

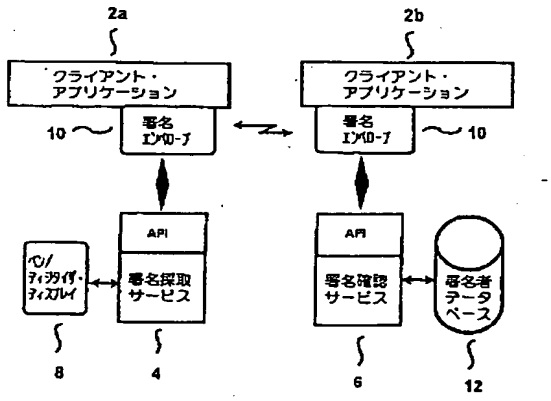

FIG. 2

【特許請求の範囲】

１．電子文書に関連する手書き署名の電子表示を作成しその後手書き署名を確認するためのコンピュータベースの方法において、

第１のコンピュータ・プロセッサにおいて、文書の画像を電子的に表示する段階、

該第１のコンピュータ・プロセッサにおいて、署名者の手書き署名を電子的に採取することによって文書に署名する段階、

該第１のコンピュータ・プロセッサにおいて、前記手書き署名に関する一揃いの計測値を署名エンベロープの中に記憶する段階、

該第１のコンピュータ・プロセッサにおいて、文書の検査合計を作成する段階、

該第１のコンピュータ・プロセッサにおいて、前記署名エンベロープの中に検査合計を記憶する段階、

該第１のコンピュータ・プロセッサにおいて、署名者の請求されたアイデンティティ（ＩＤ）を前記署名エンベロープの中に記憶する段階、

該第１のコンピュータ・プロセッサにおいて、前記署名エンベロープをコード化してコード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープを第２のコンピュータ・プロセッサへ伝送する段階、

該第２のコンピュータ・プロセッサにおいて、前記のコード化された署名エンベロープを復号する段階、

該第２のコンピュータ・プロセッサにおいて、前記署名エンベロープ内に記憶された請求されたアイデンティティをもつ人物の手書き署名の確認済みの計測値セットを検索する段階、および

該第２のコンピュータ・プロセッサにおいて、確認済みの一揃いの計測値と前記署名エンベロープ内に記憶された一揃いの計測値とを比較して類似性評点を得る段階、

を含んで成るコンピュータベースの方法。

２．前記のコード化された署名エンベロープをメモリ装置内に記憶する段階をさらに含んで成る請求の範囲第１項に記載の方法。

３．前記一揃いの計測値には平均ストローク長が含まれる請求の範囲第１項に記載の方法。

４．前記一揃いの計測値には平均ペンダウン時間が含まれる請求の範囲第１項に記載の方法。

５．前記一揃いの計測値には、加速および減速最大値の数が含まれる請求の範囲第１項に記載の方法。

６．前記一揃いの計測値には、各ストローク内の最も緩慢な点の位置合計が含まれている、請求の範囲第１項に記載の方法。

７．前記第１のプロセッサにおいて、前記署名エンベロープ内に署名の日付、時間を記憶する段階をさらに含んで成る請求の範囲第１項に記載の方法。

８．前記第１のプロセッサにおいて、前記署名エンベロープ内に前記第１のプロセッサのアイデンティティを表す標識を記憶する段階を含んで成る、請求の範囲第１項に記載の方法。

９．前記第１のプロセッサにおいて、前記手書き署名の画像の圧縮された表示を前記署名エンベロープの中に記憶する段階をさらに含んで成る、請求の範囲第１項に記載の方法。

10．前記第１のコンピュータ・プロセッサに対して類似性評点を伝送する段階をさらに含んで成る請求の範囲第１項に記載の方法。

11．第３のコンピュータ・プロセッサに対して類似性評点を伝送する段階をさらに含んで成る請求の範囲第１項に記載の方法。

12．前記第２のプロセッサにおいて、前記電子文書の第２の検査合計を作成する段階、および

前記電子文書が前記第１のコンピュータ・プロセッサで署名された文書の真正な表示であるか否かを見極めるべく電気署名エンベロープ内に記憶された検査合計に対し第２の検査合計を比較する段階、

をさらに含んで成る請求の範囲第１項に記載の方法。

13. 電子文書のための手書き署名の電子表示を作成するためのコンピュータベースの方法において、

第１のコンピュータ・プロセッサにおいて、第１の文書の画像を電子的に表示する段階、

該第１のコンピュータ・プロセッサにおいて、署名者の手書き署名を電子的に採取することによって前記第１の文書に署名する段階、

該第１のコンピュータ・プロセッサにおいて、前記手書き署名に関する一揃いの計測値を前記署名エンベロープの中に記憶する段階、

該第１のコンピュータ・プロセッサにおいて、前記第１の文書の第１の検査合計を作成する段階、

該第１のコンピュータ・プロセッサにおいて前記署名エンベロープの中に前記第１の検査合計を記憶する段階、

該第１のコンピュータ・プロセッサにおいて、前記署名エンベロープをコード化してコード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープを第２のコンピュータ・プロセッサへ伝送する段階、

該第２のコンピュータ・プロセッサにおいて、前記のコード化された署名エンベロープを復号する段階、

該第２のコンピュータ・プロセッサにおいて、第２の文書の第２の検査合計を作成する段階、および

該第２の文書が前記第１の文書の真正な表示であるか否かを見極めるべく、前記署名エンベロープ内に記憶された前記第１の検査合計に対して前記第２の検査合計を比較する段階、

を含んで成る方法。

14. 電子文書のための手書き署名の電子表示を作成するためのコンピュータベースの方法において、

第１のコンピュータ・プロセッサにおいて、第１の文書の画像を電子的に表示する段階、

該第１のコンピュータ・プロセッサにおいて、署名者の手書き署名を電子的に採取することによって第１の文書に署名する段階、

該第１のコンピュータ・プロセッサにおいて、前記手書き署名に関する一揃いの計測値を署名エンベロープの中に記憶する段階、

該第１のコンピュータ・プロセッサにおいて、第１の文書の検査合計を作成する段階、

該第１のコンピュータ・プロセッサにおいて署名署名エンベロープの中に第１の検査合計を記憶する段階、

該第１のコンピュータ・プロセッサにおいて、署名者の指示を前記署名エンベロープの中に記憶する段階、

該第１のコンピュータ・プロセッサにおいて、前記署名エンベロープをコード化してコード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープを第２のコンピュータ・プロセッサへ伝送する段階、

該第２のコンピュータ・プロセッサにおいて、前記のコード化された署名エンベロープを復号する段階、

該第２のコンピュータ・プロセッサにおいて、前記手書き署名が署名者のものであることを確認する段階、

該第２のコンピュータ・プロセッサにおいて、第２の文書の第２の検査合計を作成する段階、および

該第２のコンピュータ・プロセッサにおいて、前記第２の文書が前記第１の文書の真正な表示であるか否かを見極めるべく前記署名エンベロープ内の第１の検査合計に対して前記第２の検査合計を比較する段階、

を含んで成る方法。

15. １つの文書のための手書き署名の電子表示を作成するためのコンピュータベースの方法において、

第１の文書の画像を電子的に表示する段階、

署名者の手書き署名を電子的に採取することにより前記第１の文書に署名する

段階、

前記手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

前記第１の文書の第１の検査合計を作成する段階、

前記署名エンベロープ内に前記第１の検査合計を記憶する段階、

署名者の指示を前記署名エンベロープの中に記憶する段階、

該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープをメモリ内に記憶する段階、

該コード化された署名エンベロープを復号する段階、

前記手書き署名が署名者のものであることを確認する段階、

第２の文書の第２の検査合計を作成する段階、および

該第２の文書が前記第１の文書の真正な表示であるか否かを見極めるべく、前記署名エンベロープの中に記憶された第１の検査合計

に対して前記第２の検査合計を比較する段階、

を含んで成る方法。

16. １つの文書に関連する手書き署名の電子表示を採取し、その後手書き署名を確認するためのコンピュータベースの方法において、

署名者の手書き署名を電子的に採取することにより文書に署名する段階、

該手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

文書の検査合計を作成する段階、

署名エンベロープ内に該検査合計を記憶する段階、

署名者の請求されたアイデンティティを前記署名エンベロープの中に記憶する段階、

該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープをメモリ内に記憶する段階、

該コード化された署名エンベロープを復号する段階、

前記署名エンベロープ内に記憶されたとおりの請求されたアイデンティティをもつ人物の、この人物の確認済み手書き署名に関する確認済みの一揃いの計測値を含む署名テンプレートを、メモリから検索する段階、および

前記署名テンプレート内に記憶された確認済みの一揃いの計測値と、前記署名エンベロープ内に記憶された一揃いの計測値とを比較して、文書に署名した時点で採取された手書き署名と前記確認済みの手書き署名との間の類似度を表す類似性評点を得る段階、

を含んで成る方法。

17. 電子文書の第２の検査合計を作成する段階、および

該電子文書が、署名された文書の真正な表示であるか否かを見極めるべく、前記署名エンベロープ内に記憶された検査合計に対して第２の検査合計を比較する段階、

をさらに含んで成る、請求の範囲第16項に記載の方法。

18. １つの文書のための手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

第１のコンピュータ・プロセッサにおいて、第１の文書の画像を電子的に表示する段階、

該第１のプロセッサにおいて、第１の文書を要約するプロンプトを電子的に表示する段階、

該第１のコンピュータ・プロセッサにおいて、署名者の手書き署名を電子的に採取することによって第１の文書に署名する段階、

該第１のコンピュータ・プロセッサにおいて、署名エンベロープの中に、前記手書き署名に関する一揃いの計測値を記憶する段階、

該第１のコンピュータ・プロセッサにおいて、署名者の指示を署名エンベロープ内に記憶する段階、

該第１のプロセッサにおいて、前記署名エンベロープ内にプロンプトを記憶する段階、

該第１のコンピュータ・プロセッサにおいて、前記署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

該コード化された署名エンベロープを第２のコンピュータ・プロセッサに伝送する段階、

該第２のコンピュータ・プロセッサにおいて、前記のコード化された署名エンベロープを復号する段階、

該第２のコンピュータ・プロセッサにおいて、前記手書き署名が署名者のものであることを確認する段階、および

該第２のコンピュータ・プロセッサにおいて、前記署名エンベロープからプロンプトを検索する段階、

を含んで成る方法。

19. 前記プロンプトを表示する段階をさらに含んで成る、請求の範囲第18項に記載の方法。

20. 第１のコンピュータ・プロセッサにおいて、第１の文書の第１の検査合計を作成する段階、

該第１のコンピュータ・プロセッサにおいて、署名エンベロープ内に第１の検査合計を記憶する段階、

該第２のコンピュータ・プロセッサにおいて、第２の文書の第２の検査合計を作成する段階、および

該第２のコンピュータ・プロセッサにおいて、該第２の文書が前記第１の文書の真正な表示であるか否かを見極めるべく前記署名エンベロープ内に記憶された第１の検査合計に対して前記第２の検査合計を比較する段階、

をさらに含んで成る、請求の範囲第18項に記載の方法。

21. １つの文書のための手書き署名の電子表示を作成し確認するためのコンピュータベースの方法において、

第１の文書の画像を電子的に表示する段階、

該第１の文書の性質を識別する重要プロンプトを電子的に表示する段階、

署名者の手書き署名を電子的に採取することによって該第１の文書に署名する

段階、

該手書き署名に関連する一揃いの計測値を署名エンベロープの中に記憶する段階、

該署名エンベロープ内に、署名者の請求されたアイデンティティの指示を記憶する段階、

該署名エンベロープ内に重要プロンプトを記憶する段階、

該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

その後、該コード化された署名エンベロープを復号する段階、

前記手書き署名が署名者のものであることを確認する段階、および

署名者が前記第１の文書の性質についての情報提供を受けたことを確かめるため前記署名エンベロープから重要プロンプトを検索する段階、

を含んで成る方法。

22. 前記コンピュータベースの方法には、さらに、重要プロンプトを表示する段階が含まれている、請求の範囲第21項に記載の方法。

23. 前記手書き署名が署名者のものであることを確認する段階にはさらに、

前記署名エンベロープ内に記憶されているような署名者の請求されたアイデンティティをもつ人物の、この人物の確認済み署名の確認済み測定値を含む署名テンプレートを、メモリから検索する段階、

前記第１の文書の署名の時点で採取された手書き署名と確認された手書き署名の間の類似度を表す類似性評点を決定する段階、

が含まれている、請求の範囲第21項に記載の方法。

24. クライアント・アプリケーションの要請があった時点で、該クライアント・アプリケーションに対して類似性評点を伝送する段階をさらに含んで成る、請求の範囲第23項に記載の方法。

25. クライアント・アプリケーションに対して類似性評点を伝送す

る段階、および

該クライアント・アプリケーションに対して重要プロンプトを伝送する段階、をさらに含んで成る請求の範囲第23項に記載の方法。

26. 前記第１の文書の第１の検査合計を作成する段階、

前記署名エンベロープ内に第１の検査合計を記憶する段階、

メモリ内に前記署名エンベロープを記憶する段階、

第２の文書の第２の検査合計を作成する段階、および

該第２の文書が前記第１の文書の真正な表示であるか否かを見極めるべく、前記署名エンベロープ内の第１の検査合計に対して前記第２の検査合計を比較する段階、

をさらに含んで成る請求の範囲第23項に記載の方法。

27. クライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で、１つの文書のための手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

前記クライアント・アプリケーションの制御下で、

ａ．第１の文書の画像を表示する段階、

ｂ．前記署名採取アプリケーションが手書き署名を採取することを要請する段階、

ｃ．前記署名採取アプリケーションへと、第１の文書に関連するメッセージである重要プロンプトを移行させる段階、

前記署名採取アプリケーションの制御下で、

ｄ．署名採取ウィンドウを表示する段階、

ｅ．重要プロンプトを表示する段階、

ｆ．ユーザーの手書き署名を電子的に採取することによって第１の文書にユーザーが署名できるようにする段階、

ｇ．該手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

ｈ．ユーザーの請求されたアイデンティティの指示を該署名エンベロープ内に記憶する段階、

ｉ．該署名エンベロープ内に前記重要プロンプトを記憶する段階、

ｊ．該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

ｋ．前記クライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、

前記クライアント・アプリケーションの制御下で、

ｌ．前記のコード化された署名エンベロープを前記署名確認アプリケーションへと移行させる段階、および

前記署名確認アプリケーション制御下で、

ｍ．前記のコード化された署名エンベロープを復号する段階、

ｎ．請求されたアイデンティティが署名エンベロープ内に記憶されているユーザーの確認済み手書き署名に対応する確認済みの一揃いの計測値を含むテンプレートをデータベースから検索する段階、

ｏ．前記署名エンベロープ内に記憶された一揃いの計測値をテンプレート内の確認済みの一揃いの計測値と比較して類似性評点を得る段階、

ｐ．該署名エンベロープから前記重要プロンプトを検索する段階、および

ｑ．該重要プロンプトと類似性評点を前記クライアント・アプリケーションへと移行させる段階、

を含んで成る方法。

28．前記署名採取アプリケーションの制御下で、前記第１の文書の

第１の検査合計を作成し、前記署名エンベロープ内の第１の検査合計を記憶する段階、および

前記署名確認アプリケーションの制御下で、第２の文書の第２の検査合計を作成し、該第２の文書が前記第１の文書の真正な表示であるか否かを見極めるべく前記署名エンベロープ内に記憶された第１の検査合計に対して前記第２の検査合計を比較する段階、

をさらに含んで成る請求の範囲第27項に記載の方法。

29．前記署名採取アプリケーションが第１のコンピュータ・プロセッサ上で実行

され、前記署名確認アプリケーションが第２のコンピュータ・プロセッサ上で実行される、請求の範囲第27項に記載の方法。

30. 前記一揃いの計測値には平均ストローク長が含まれる請求の範囲第27項に記載の方法。

31. 前記一揃いの計測値には平均ペンダウン時間が含まれる請求の範囲第27項に記載の方法。

32. 前記一揃いの計測値には、加速および減速最大値の数が含まれる請求の範囲第27項に記載の方法。

33. 前記一揃いの計測値には、各ストローク内の最も緩慢な点の位置合計が含まれている、請求の範囲第27項に記載の方法。

34. 前記署名採取アプリケーションの制御下で、前記署名エンベロープ内に署名の日付、時間を記憶する段階をさらに含んで成る請求の範囲第27項に記載の方法。

35. 前記署名採取アプリケーションの制御下で、前記署名エンベロープ内にクライアント・アプリケーションを実行しているコンピュータ・プロセッサのアイデンティティを表す標識を記憶する段階を含んで成る、請求の範囲第27項に記載の方法。

36. 前記署名採取アプリケーションの制御下で、手書きの署名の画

像の圧縮された表示を前記署名エンベロープの中に記憶する段階をさらに含んで成る、請求の範囲第27項に記載の方法。

37. 前記署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮されたビットマップ表示を前記署名エンベロープ内に記憶する段階をさらに含んで成る、請求の範囲第27項に記載の方法。

38. クライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

前記クライアント・アプリケーションの制御下で、

ａ. 前記署名採取アプリケーションが手書き署名を採取することを要請する段

階、

前記署名採取アプリケーションの制御下で

ｂ．ユーザーが手書き署名を電子的に入力できるようにする段階、

ｃ．ユーザーの手書き署名を電子的に採取する段階、

ｄ．該手書き署名に関係する一揃いの計測値を算出する段階、

ｅ．署名エンベロープ内に前記手書き署名に関係する一揃いの計測値を記憶する段階、

ｆ．ユーザーの請求されたアイデンティティの指示を前記署名エンベロープ内に記憶する段階、

ｇ．前記署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

ｈ．クライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、

前記クライアント・アプリケーションの制御下で、

ｉ．前記のコード化された署名エンベロープを前記署名確認アプリケーションへと移行させる段階、および

前記署名確認アプリケーションの制御下で、

ｊ．前記のコード化された署名エンベロープを復号する段階、

ｋ．請求されたアイデンティティが前記署名エンベロープ内に記憶されているユーザーの確認済み手書き署名に対応する確認済みの一揃いの計測値を含むテンプレートをデータベースから検索する段階、

ｌ．該署名エンベロープ内に記憶された一揃いの計測値をテンプレート内の確認済み一揃いの計測値と比較して類似性評点を得る段階、

ｍ．該類似性評点を前記クライアント・アプリケーションへと移行させる段階、

を含んで成る方法。

39．前記クライアント・アプリケーションの制御下で、類似性評点を用いて、ユーザーがコンピュータシステム内の単数または複数のアプリケーションに対して

アクセスできるか否かを見極める段階をさらに含んで成る、請求の範囲第38項に記載の方法。

40. 前記クライアント・アプリケーションの制御下で、ユーザーがクレジットで商品を購入できるか否かを見極めるべく前記類似性評点を利用する段階をさらに含んで成る、請求の範囲第38項に記載の方法。

41. 前記署名採取アプリケーションが第１のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第２のコンピュータ・プロセッサ上で実行される請求の範囲第38項に記載の方法。

42. 前記一揃いの計測値には平均ストローク長が含まれる請求の範囲第38項に記載の方法。

43. 前記一揃いの計測値には平均ペンダウン時間が含まれる請求の範囲第38項に記載の方法。

44. 前記一揃いの計測値には、加速および減速最大値の数が含まれる請求の範囲第38項に記載の方法。

45. 前記一揃いの計測値には、各ストローク内の最も緩慢な点の位置合計が含まれている、請求の範囲第38項に記載の方法。

46. 前記署名採取アプリケーションの制御下で、署名エンベロープ内に署名の日付、時間を記憶する段階をさらに含んで成る請求の範囲第38項に記載の方法。

47. 前記署名採取アプリケーションの制御下で、前記署名エンベロープ内に前記クライアント・アプリケーションを実行しているコンピュータ・プロセッサのアイデンティティを表す標識を記憶する段階を含んで成る、請求の範囲第38項に記載の方法。

48. 前記署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮された表示を前記署名エンベロープの中に記憶する段階をさらに含んで成る、請求の範囲第38項に記載の方法。

49. 前記署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮されたビットマップ表示を前記署名エンベロープ内に記憶する段階をさらに含んで成る、請求の範囲第38項に記載の方法。

50. クライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で、１つの電子文書上の手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

前記クライアント・アプリケーションの制御下で、

ａ．文書の画像を表示する段階、

ｂ．前記署名採取アプリケーションが手書き署名を採取することを要請する段階、

前記署名採取アプリケーションの制御下で、

ｃ．ユーザーが手書き署名を電子的に入力できるようにする段階、

ｄ．ユーザーの手書き署名を電子的に採取する段階、

ｅ．該手書き署名に関係する一揃いの計測値を算出する段階、

ｆ．該手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

ｇ．ユーザーの請求されたアイデンティティの指示を該署名エンベロープ内に記憶する段階、

ｈ．文書の検査合計を作成する段階、

ｉ．前記署名エンベロープ内に検査合計を記憶する段階、

ｊ．該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

ｋ．前記クライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、

前記クライアント・アプリケーションの制御下で、

ｌ．前記のコード化された署名エンベロープを前記署名確認アプリケーションへと移行させる段階、および

前記署名確認アプリケーションの制御下で、

ｍ．前記のコード化された署名エンベロープを復号する段階、

ｎ．請求されたアイデンティティが前記署名エンベロープ内に記憶されているユーザーの確認済み手書き署名に対応する確認済みの一揃いの計測値を含むテン

プレートをデータベースから検索する段階、

ｏ．前記署名エンベロープ内に記憶された一揃いの計測値をテンプレート内の確認済み一揃いの計測値と比較して類似性評点を得る段階、および

ｐ．該類似性評点を前記クライアント・アプリケーションへと移行させる段階、

を含んで成る方法。

51．クライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で、１つの電子文書上の手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

前記クライアント・アプリケーションの制御下で、

ａ．第１の文書の画像を表示する段階、

ｂ．前記署名採取アプリケーションが手書き署名を採取することを要請する段階、

前記署名採取アプリケーションの制御下で、

ｃ．ユーザーが手書き署名を電子的に入力できるようにする段階、

ｄ．ユーザーの手書き署名を電子的に採取する段階、

ｅ．該手書き署名に関係する一揃いの計測値を計算する段階、

ｆ．該手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

ｇ．第１の文書の第１の検査合計を作成する段階、

ｈ．前記署名エンベロープ内に検査合計を記憶する段階、

ｉ．該署名エンベロープをコード化して、コード化された署名エンベロープを作成する段階、

ｊ．前記クライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、

前記クライアント・アプリケーションの制御下で、

ｋ．前記のコード化された署名エンベロープを前記署名確認アプリケーションへと移行させる段階、および

前記署名確認アプリケーションの制御下で、

ｌ．前記のコード化された署名エンベロープを復号する段階、

ｍ．第２の文書の第２の検査合計を作成する段階、

ｎ．前記第１の文書が該第２の文書と同じであるか否かを確かめ

るべく前記第２の検査合計に対して前記署名エンベロープ内に記憶された第１の検査合計を比較する段階、および

ｏ．前記第１の文書が前記第２の文書と同じであるか否かを前記クライアント・アプリケーションに情報提供する段階を含んで成る方法。

52．前記署名採取アプリケーションが第１のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第２のコンピュータ・プロセッサ上で実行される、請求の範囲第51項に記載の方法。

53．前記一揃いの計測値には平均ストローク長が含まれる請求の範囲第51項に記載の方法。

54．前記一揃いの計測値には平均ペンダウン時間が含まれる請求の範囲第51項に記載の方法。

55．前記一揃いの計測値には、加速および減速最大値の数が含まれる請求の範囲第51項に記載の方法。

56．前記一揃いの計測値には、各ストローク内の最も緩慢な点の位置合計が含まれている、請求の範囲第55項に記載の方法。

57．前記署名採取アプリケーションの制御下で、前記署名エンベロープ内に署名の日付、時間を記憶する段階をさらに含んで成る請求の範囲第51項に記載の方法。

58．前記署名採取アプリケーションの制御下で、前記署名エンベロープ内に前記クライアント・アプリケーションを実行しているコンピュータ・プロセッサのアイデンティティを表す標識を記憶する段階を含んで成る、請求の範囲第51項に記載の方法。

59．署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮された表示を前記署名エンベロープの中に記憶する段階をさらに含んで成る、請求の範囲

第58項に記載の方法。

60. 前記署名採取アプリケーションの制御下で、手書きの署名の画像の圧縮されたビットマップ表示を前記署名エンベロープ内で記憶する段階をさらに含んで成る、請求の範囲第51項に記載の方法。

61. 第１のクライアント・アプリケーション、第２のクライアント・アプリケーション、署名採取アプリケーションおよび署名確認アプリケーションをもつコンピュータシステム内で、手書き署名の電子表示を採取し確認するためのコンピュータベースの方法において、

前記第１のクライアント・アプリケーションの制御下で、

ａ．前記署名採取アプリケーションが手書き署名を採取することを要請する段階、

前記署名採取アプリケーションの制御下で

ｂ．ユーザーが手書き署名を電子的に入力できるようにする段階、

ｃ．ユーザーの手書き署名を電子的に採取する段階、

ｄ．該手書き署名に関係する一揃いの計測値を計算する段階、

ｅ．該手書き署名に関係する一揃いの計測値を署名エンベロープ内に記憶する段階、

ｆ．ユーザーの請求されたアイデンティティの指示を該署名エンベロープ内に記憶する段階、

ｇ．該署名エンベロープをコード化して、コード化された署名エンベロープを生成する段階、

ｈ．前記第１のクライアント・アプリケーションへと該コード化された署名エンベロープを移行させる段階、

前記第１のクライアント・アプリケーションの制御下で、

ｉ．前記のコード化された署名エンベロープを前記第２のクライアント・アプリケーションへと移行させる段階、

前記第２のクライアント・アプリケーションの制御下で

ｊ．前記のコード化された署名エンベロープを署名確認アプリケ

ーションへと移行させる段階、および

前記署名確認アプリケーションの制御下で、

ｋ．前記のコード化された署名エンベロープを復号する段階、

ｌ．請求されたアイデンティティが前記署名エンベロープ内に記憶されているユーザーの確認済み手書き署名に対応する確認済みの一揃いの計測値を含むテンプレートをデータベースから検索する段階、

ｍ．前記署名エンベロープ内に記憶された一揃いの計測値をテンプレート内の確認済み一揃いの計測値と比較して類似性評点を得る段階、および

ｎ．該類似性評点を前記第２のクライアント・アプリケーションへと移行させる段階、

を含んで成る方法。

62．前記第２のクライアント・アプリケーションの制御下で、前記類似性評点を利用して、ユーザーがコンピュータシステム内の単数または複数のアプリケーションおよびデータにアクセスできるか否かを見極める段階をさらに含んで成る、請求の範囲第61項に記載の方法。

63．前記第２のクライアント・アプリケーションの条件下で、ユーザーがクレジットで商品を購入できるか否かを見極めるべく前記類似性評点を利用する段階をさらに含んで成る、請求の範囲第61項に記載の方法。

64．前記署名採取アプリケーションが第１のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第２のコンピュータ・プロセッサ上で実行される、請求の範囲第61項に記載の方法。

65．前記第１のクライアント・アプリケーションが第１のコンピュ

ータ・プロセッサ上で実行され、前記第２のクライアント・アプリケーションが第２のコンピュータ・プロセッサで実行される、請求の範囲第61項に記載の方法。

66．前記第１のコンピュータ・プロセッサが第１のオペレーティングシステムに従って動作し、前記第２のコンピュータ・プロセッサが第２のオペレーティングシステムに従って動作する、請求の範囲第65項に記載の方法。

67. 前記署名採取アプリケーションが第１のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第２のコンピュータ・プロセッサ上で実行される、請求の範囲第65項に記載の方法。

68. 前記署名採取アプリケーションが第３のコンピュータ・プロセッサ上で実行され、前記署名確認アプリケーションが第４のコンピュータ・プロセッサ上で実行される、請求の範囲第65項に記載の方法。

69. 電子文書のための手書き署名の電子表示を作成するためのコンピュータベースのシステムにおいて、

署名者の手書き署名を電子的に採取することにより、署名者が第１の文書に署名できるようにするための手段、

署名エンベロープ内に、該手書き署名に関係する一揃いの計測値を記憶するための手段、

前記第１の文書の第１の検査合計を作成するための手段、

前記署名エンベロープ内に前記第１の検査合計を作成するための手段、

署名者の指示を前記署名エンベロープ内に記憶するための手段、および

該署名エンベロープをコード化して、コード化された署名エンベロープを作成するための手段、

を含んで成るシステム。

70. 前記のコード化された署名エンベロープを復号するための手段、

該署名エンベロープ内に記憶されている手書き署名が署名者のものであることを確認するための手段、

第２の文書の第２の検査合計を作成するための手段；および

該第２の文書が前記第１の文書の真正な表示であるか否かを見極めるべく前記署名エンベロープ内に記憶された第１の検査合計に対して前記第２の検査合計を比較するための手段、

をさらに含んで成る、請求の範囲第69項に記載のシステム。

71. 前記のコード化された署名エンベロープをメモリ内に記憶するための手段をさらに含んで成る、請求の範囲第70項に記載のシステム。

72. 第１のプロセッサに手書き署名を電子的に入力するための手段、

署名者の手書き署名を電子的に採取するための手段、

署名エンベロープ内に該手書き署名に関係する一揃いの計測値を記憶するための手段、

署名者の請求されたアイデンティティを入力するための手段、

前記署名エンベロープ内に署名者の請求されたアイデンティティを記憶するための手段、

前記署名エンベロープをコード化して、コード化された署名エンベロープを作成する手段、および

該コード化された署名エンベロープを遠隔の署名確認センターに通信するための手段、

を含む、前記手書き署名を採取するための複数の第１のプロセッサ、および

前記第１のプロセッサの１つからコード化された署名エンベロープを受理するための手段、

該コード化された署名エンベロープを復号するための手段、

確認済みの一揃いの署名計測値を含み署名者の請求されたアイデンティティに対応する署名テンプレートを検索するべくデータベースをアクセスするための手段、

前記確認済みの一揃いの署名計測値と、前記署名エンベロープ内に記憶された一揃いの計測値とを比較することによって前記手書き署名を確認するための手段、

前記署名エンベロープ内に記憶された一揃いの計測値と前記確認済みの一揃いの署名計測値との間の類似性を表す類似性評点を決定するための手段、

前記第１のプロセッサの１つに対して該類似性評点を通信するための手段

を含み前記署名テンプレートのデータベースに結合された第２のプロセッサによって制御され、複数の第１のプロセッサの各々との関係において遠隔に位置づけられているもののそれに対し電子的に結合されている署名確認センター、

を含んで成る、署名確認センターシステム。

73. 第１のプロセッサに手書き署名を電子的に入力するための手段、

署名者の手書き署名を電子的に採取するための手段、

署名エンベロープ内に該手書き署名に関係する一揃いの計測値を記憶するための手段、

署名者の請求されたアイデンティティを入力するための手段、

前記署名エンベロープ内に署名者の請求されたアイデンティティを記憶するための手段、

該署名エンベロープをコード化して、コード化された署名エンベ

ロープを作成する手段、および

該コード化された署名エンベロープを遠隔の署名確認センターに通信するための手段、

を含む、手書き署名を採取するための複数の第１のプロセッサ、

署名者についての確認済みの一揃いの署名計測値を含み各々の署名者のアイデンティティにより指標付けされた複数の署名テンプレートを含む確認済みの手書き署名データを記憶するための中央データベース、

前記第１のプロセッサの１つからコード化された署名エンベロープを受理するための手段、

該コード化された署名エンベロープを復号するための手段、

署名者の請求されたアイデンティティに対応する署名テンプレートを検索するべく前記中央データベースをアクセスするための手段、

前記確認済みの一揃いの署名計測値と、前記署名エンベロープ内に記憶された一揃いの計測値とを比較することによって前記手書き署名を確認するための手段、

前記署名エンベロープ内に記憶された一揃いの計測値と前記確認済みの一揃いの署名計測値との間の類似性を表す類似性評点を決定するための手段、

前記第１のプロセッサの１つに対して該類似性評点を通信するための手段

を含み前記署名テンプレートの中央データベースに結合された第２のプロセッサによって制御され、前記複数の第１のプロセッサの各々との関係において遠隔に

位置づけられているもののそれに対し電子的に結合されている署名確認センター
、
を含んで成る、署名確認センターシステム。

【発明の詳細な説明】

手書き署名を採取し、記憶し、伝送し、および、認証する方法ならびにそのシステム

発明の分野

本発明は手書き署名を電子方式で記憶保存する方法およびシステムに関し、より詳しくは、電子方式で記憶した手書き署名、および、それに関連する文書の確認を複数のプラットフォーム（Platform）で実施可能にする方法およびシステムに関するものである。

発明の背景

机上設置型にしろ携帯型にしろ、電子ペンまたはディジタイザによるデータ入力を可能にした多くのコンピュータシステムが設計されている。手書きの字句を認識し、標準テキストに翻訳するソフトウェアも世に出ている。また、電子ペン入力を利用したアプリケーションも数多く存在している。ペン入力は、コンピュータキーボードに馴染みのない人や苦手な人にもコンピュータを楽に使用できるようにしている。さらに、ペン入力型コンピュータの使用、ディジタル形式による情報の記憶、およびその伝送は、紙の使用を減らしまたはそれを廃止するといったような重要な商業上の利益を実現している。

ディジタイザは、典型的に、ペン先の位置を１秒間に約１００回サンプルし、そして一インチの７０分の一の動きを感知する感度を有している。したがって、ディジタイザは人間の手の動きを極めて正確に記録することができる。コンピュータによる署名確認はこの点を利用して目に見える署名の形だけではなく、署名の速さおよび書くリズム等の署名の動的な面を分析することができる。

ペン入力（例えば、手書き署名）を取り込み、ペン入力の基本的な特徴を決定し、そしてそのペン入力を電子方式で表すことを可能にするアルゴリズムがある。また、電子方式の手書き署名が同一人のものか否かを決定することができるアルゴリズムもある。これらは、例えば米国特許第5,109,426号（英国特許出願第9 0 24393.3号）、米国特許第4,495,644号、および英国特許出願第1480066号等に開示されているが、ここでの詳細な説明は省略する。

署名の確認は、コンピュータの安全性に対し非常に重要な貢献をすることができる。コンピュータの他の全ての安全機構は、個人のみが知る事項（例えば、パスワード）、または所有する物（例えば、物理的なキー）に依存している。署名の確認は、このようなものに頼る代わりに、盗難または漏洩の心配のない身体の動作の様子に依存することによって、コンピュータ使用者の真の同一性に関する確実な証拠を提供する。

現在まで署名の確認は、主としてアクセス領域の安全性の観点から、コンピュータシステムの全てまたは一部に対する使用者のアクセスを許す前に、本人であることを確認する目的で採用されてきた。

しかし、紙に書く伝統的な署名は、契約書あるいは遺言書に署名

するとか、為替を切る際には支払い拒否に対抗するための保護手段として署名するといったように、種々の意志または意図を証明するのに使用されている。

コンピュータ化された書類の利用が可能になっているにも拘わらず、紙面への署名に対する法的、または文化的要求から、今日でもなお多くの分野で紙に依存することが必要である。

したがって、ディジタル形式、即ち電子方式の文書よりも、それと同じハードコピーの方が好まれる場合がしばしば生じている。例えば、土地譲渡に関する遺言書とか契約書は、殆ど全ての司法管轄区域における法律によって、それが手書きであること、およびその書面に対する当事者並びに証人の手書き署名原本を含んでいることが要求される。文書が電子方式で作成されている場合、文書の内容を比較的簡単に改竄できるため、後日見る書面が最初に作成された物と同一であるかが不確かであることが多い。ペン入力機能を使用して取り込んだ手書き署名

は文書のテキストに組み入れることはできるが、後日見る文書が“電子的に”署名されたものであるかは、決して確かとはいえない。

したがって、手書き署名の採取（Capture）および確認の科学を安全アクセス機構としてより、もっと広範な面に適用することが望ましいだろう。特に、ある意図（例えば、法的文書に署名したことの意図）を証明する領域においては、署名された文書とその署名者の署名とを関連付ける確実な署名採取および確認方法が必要になる。

現存のシステムは、電子方式による署名がその後改竄されたかどうか、そして電子文書に関連するその電子方式の署名がその文書の処理（作成）時点で採取されたどうかに焦点を当ててきた。例えば、キャップ（Kapp）等に付与された米国特許第5,195,133号は、商業上の責務を認めるという趣旨の署名が問題処理（文書作成）時点で

行われ、そしてその署名が他の問題処理に関して採られた本物の署名ではなく、またその処理に関するディジタル記録に詐欺的に組み込まれたものではないことを保証する機構について述べている。このキャップ等によるシステムと同様なシステムは、処理に関するディジタル記録を作成し、その処理時点でなされた署名のディジタル表示を採取し、処理のディジタル記録を使用して署名のディジタル表示を記号化している。この方法は、署名の表示が、署名したといわれている時点で署名されたものであることを保証することをその目的としてる。しかし、このような手法はディジタル形式で採取した手書き署名が後で修正されたかどうかについては確認がとれない。さらに、キャップ等による手法に見られるようなシステムは処理（文書作成）を必要とするから、処理を伴わない環境下で署名を採り、確認するという操作は不可能である。

現存の手書き署名の採取および確認システムは、単一のプラットフォームで使用するように構成されている。手書きの署名を符号化して、他のアプリケーションが電子方式の手書き署名を利用できないようにすることがしばしば行われる。しかし、インターネットを含む今日の進歩したコンピュータ間通信のおかげで、多くのアプリケーションは、署名が行われたときと同じ機器または同じ時間に確

認をすることを要求しないだろう。例えば、手書き署名を一つの装置で電子的に採取し、記憶し、もう他のコンピュータ・プラットフォームに電子的に伝送し、その後で確認するシステムが望ましい。したがって、統合されたプラットフォーム間署名確認システムが必要になる。特に、特定の基礎となるハードウェアを前提とせず、かつ異種のコンピュータおよび異種のオペレーションシステム間で移動が可能なシステムが必要である。

多くの業務機関および政府機関の部局が、文書に署名を求めるこ

とはよくあることである。例えば、小切手またはクレジットカードで物を買うとき、レンタカーの契約をするとき、リース契約をするとき、運転者登録またはその他の政府許可を申請するとき、選挙の日、または試験の受験証明等々である。また、署名を求める人が、署名を求められた個人を熟知せず、要請に基づいてした署名を対比照合するその署名者の本物の署名を持ち合わせていない、といったことはよくあることである。さらに、照合のために本物の署名が用意されていたとしても、署名を要求する者が、二つの署名が同一人によるものかどうかの判定に未熟であったりすることもよくあることである。したがって、一つの場所で署名を採取し、それを多くの個人に関する確認済みの署名行動を記録している中央局に電気的に伝送し、そして署名者の身元確認を署名地に返すシステムが必要である。

また、ある場合には、契約書またはその他の法的書類に署名した者が後日、署名した文書の性質を理解していなかったこと、または彼または彼女が文書に署名したときに誤解させられたことを主張して、彼または彼女の責務を終了させようとすることがある。さらに、マルチウインドウコンピュータ環境下では、電子的に文書に署名した者が、実際に署名したコンピュータのどの文書に記録されているかが不確かになるかもしれない。もし記録が署名時点でなされたとすれば（それは後から取り出せる）、文書に署名する際に署名人が何を告げられたかを記録し、署名する前に、これから署名する文書の正体、性質、および重要性に関して署名人に警告することが有用である。

要するに、署名採取が必要とされる多様な環境において、手書き署名採取およ

び確認技術の応用を可能にすることによって、電子ペン入力装置の高まりつつある利用性を用いるシステムが必要である。

発明の要約

したがって、本発明は手書き署名を電子的に採取し、この署名を電子方式で記憶し、採取した手書き署名を伝送し、そして採取した手書き署名を認証するための方法およびそのシステムを提供するものである。

本願において使用する“署名”という表現は、その意志または同意を表す者によってなされた手書きの標し（マーク）を意味するものとする。そして、この言葉は通常その者の自署と考えられるものを含んでいる。また、“署名した、または署名された”という表現は、署名に対応する意味を有し、その書き物を認証する意図を持つ当事者によって書かれ、または採用された如何なる記号も含むものとする。その場合、その書き物は電子方式によるのものであってもよい。ただし、本願において使用する“署名”は、以下のものを含まないことに注意されたい。即ち、“ディジタル署名”としてコンピュータ科学の分野で知られるようになったもの、言い換えれば、電子文書を作成し、または伝送する本人を確定する電子コードを含まない。“ディジタル署名”は、手書き署名を、特定の個人に与えられかつ秘密に保持しなければならない暗唱英文字数字“キー”でもって置き換える機能を有している。これとは対照的に、本発明は人の手書き署名を電子的に採取し、かつ、処理することを指向するものである。

本発明の代表的な実施例では、公知の電子ペンベースのハードウェアを利用して、手書き署名を電子的に採取している。

本発明の代表的な実施例は、署名採取モジュール、署名確認モジュール、およびテンプレート（Template）・データベースを含んでいる。

署名採取モジュールは本人の署名を採取し、その署名行為を示す（または記録する）署名エンベロープ（署名包袋）を作る。署名エンベロープは電子方式、例えば電子ペンベースのコンピュータスクリーン上で採取された署名の手書きに関連する一定のデータを記録する。典型的には、署名採取モジュールはクライアン

ト・アプリケーションによって呼び出され、制御され、そしてこれと通信を行う。

例えば、クライアント・アプリケーションは文書に関する手書き署名を要求することができる。クライアント・アプリケーションが署名採取モジュールを呼び出すと、このモジュールはコンピュータスクリーン上に署名採取用ウインドウを表示して、クライアントに対し当該コンピュータスクリーン上の署名採取用ウインドウに彼または彼女の署名（例えば、電子鉄筆を使用して）を書くことを要求する。これに対して、クライアント・アプリケーションは署名採取モジュールに対して、署名した文書の識別記号、そして／または文書に署名した理由（または文書の重要性）を送る。重要プロンプト（グラビティ・プロンプト：Gravity Prompt）と称するこの情報は、使用者に対し署名採取モジュールによって署名採取ウインドウに示される。この表示によって使用者は、署名されている文書が彼または彼女が署名したと思う文書を確認でき、さらに使用者に署名行為の理由およびその重要さを警告する。

使用者が文書に署名するとき（例えば、ペンまたは鉄筆をスクリーン上に走らせて）、鉄筆の移動軌跡を描く画像（イメージ）が現れる。したがって、使用者の署名（即ち、自署）が使用者に対して表示される。署名時、署名採取モジュールは署名行為に関してある一定の特色、例えば署名の大きさ、曲線の形状と相対的位置、ループ、直線、点、斜線、その他書いた署名の特色と共に、署名に特色を与える相対速度等を測定する。これらの測定は“署名行為統計”

（Act-of-signing Statistics）”と呼ぶことができる。

本発明による代表的実施例では、署名採取モジュールは署名された文書の検査合計値（Checksum）を作成する。この文書の検査合計値は、署名した申立てを受けている文書が、確かに署名されたこと、さらにこの文書に何ら変更が加えられていなかったことを後日確認するのに使用することができる。

代表的な実施例では、文書の検査合計値は文書原本の完全な陳述書を構成するものではなく、同原本をこの文書の検査合計値から起こすことはできない。文書の検査合計値は文書に対して数学的関係を持っている。もし文書が変更されると

、文書はもはや検査合計値に対して数学的整合性を維持することができなくなる。

上記実施例に代わる実施例では、文書の検査合計値に加えて、あるいはそれに代わるものとして、署名された文書の圧縮表示を作成することが可能である。

署名採取モジュールはデータ、中でも署名行為統計、署名の日時、署名人請求の識別記号、重要プロンプトに現れる言葉、文書検査合計値、そして選択的には、署名の図形画像を示すデータをコード化する。そして、この署名採取モジュールはこれらコード化データを含む署名エンベロープを作成する。代表的実施例では、署名エンベロープはコード化文字列データとなる。したがって、この署名エンベロープは書込み時点における諸事項を示すための確実な方法である。

また、代表的な実施例によれば、クライアント・アプリケーションが署名エンベロープに含まれている情報を解読したりまたは変更したりすることはできない。

署名確認モジュールは、特定の署名が本物である確率を報告する。署名確認モジュールはテンプレート・データベースにアクセスする

ことができる。このテンプレート・データベースは複数のテンプレートを記憶している。各テンプレートは個人の署名行為統計と、その個人に関する既知の識別記号とを含んでいる。各テンプレートは、制御された登録処理過程を介して作成され、そして後日のアクセス用としてテンプレート・データベースに記憶される。

代表的な実施例では、署名確認モジュールおよびテンプレート・データベースは、多くのクライアント・アプリケーションからアクセスできる離れた位置にある。例えば、署名確認モジュールとテンプレート・データベースは、独立した中央署名確認局に設けられる。これに代わる他の実施例では、上記の署名確認モジュールとテンプレート・データベースは、必要に応じてクライアント・アプリケーションからアクセスできる局部システムに設けられる。

クライアント・アプリケーションが署名確認をするとき、クライアント・アプリケーションは確認対象署名の署名エンベロープを署名確認モジュールに送る。

各クライアント・アプリケーションは、そのクライアント・アプリケーションによって作成された署名、またはその他のクライアント・アプリケーションによって以前に作成した署名を確認することができる。

例えば、署名採取モジュールを多くのコンピュータ、例えばペン書込みベースのポータブルコンピュータに内蔵させ、一つのホストコンピュータに署名確認モジュールを設けることもできる。ポータブルコンピュータはいつでも多くの署名を採取して（したがって、多くの署名エンベロープを作成し）、それを署名確認用のホストコンピュータに伝送する。

署名確認モジュールが特定の署名エンベロープを受けたときに、この署名確認モジュールは、上記の署名エンベロープが同署名エンベロープにて識別されている使用者による真の署名書き込み時に作

成されたものかどうかを評価するよう署名確認モジュールに指示することができる。署名確認モジュールは署名エンベロープを解読し、当該署名エンベロープに含まれている情報と、テンプレート・データベースに記憶されている署名テンプレートとを比較することができる。この比較に基づいて、署名確認モジュールは署名の整合性に関する百分率（例えば、７８％）を決定し、この百分率および署名エンベロープに記憶されているその他の情報をクライアント・アプリケーションに報告する。

したがって、本発明は電子的に採取した手書き署名を、これまでの紙を用いた署名と同じように使用することを可能にするものである。本発明によって採取された署名は、偽造および詐欺行為の検出および防止を支援するコンピュータ技術によって、伝統的な紙に書く署名の持つ「性能」を凌ぐであろう。

本発明は、現存のソフトウェアプログラムと共に使用できるように設計されている。例えば他のコンピュータプログラムによって作動するソフトウェア要素として使用できるように設計されている。また、本発明は使用者のコンピュータネットワークへのアクセスを可能にする防護安全プログラムの一部として、ワードプロセッサの一部として、あるいは電子メールプログラム（Ｅ－メールプログラム）の一部として（例えば、Ｅ－メールメッセージ発信人の識別記号確認に）使

用することができる。本発明は特に署名の採取および確認に関係する処理を行う。（ここで用いられているように、本発明によるモジュールを利用するプログラムを「クライアント・プログラム」という）。

したがって、クライアント・プログラムは本発明を用いてあらゆる目的のために署名を採取することができる。本発明は同意を示す伝統的なやり方（署名）を新たな技術環境に進展させると共に、紙

使用の必要性をなくすことできる。例えば、本発明による署名採取モジュールは、ディジタイザが取り付けられているケーブルテレビの変換ユニット（時には「セットートップボックス(set-top box)」と言われる）に内蔵させることができるから、視聴者は本発明を用いて種々の物品およびサービスの供給権限をその供給者に与えることができる。そこで採取された署名は供給者のシステムに伝送され、そこで物品、サービスの配送前に署名確認モジュールに送ることができ、事柄（取引：Event）の記録として保管される。この方法の利点は家族構成員めいめいが個人のカードを持ち歩いたり、それに“暗証番号”を付けたりすることをせずに、個人化（例えば、親、子供等）ができる点である。また、署名採取モジュールを例えば、裏面に適当なタッチセンサ式ディジタイザを取り付けた手持ち型の遠隔制御ユニットに設ければ、本発明の能力は容易に高められる。

もう一つの例は、車販売店で車を買うためにローンを組む場合である。手書き署名は署名採取モジュールによって採取することができる。この結果として生じた署名エンベロープは独立の署名確認局に送付される。この確認局から返されてきた確認記録を使って、車が買い手の手に渡る前に、全体のクレジット査定が計算される。

また、署名はそれに続く確認を要しない場合とか、ある個人がした署名がその受取人にとって初めてのものである場合にも採られる。例えば、新郎新婦による結婚許可宣誓書への署名、客によるホテル登録用紙への署名、および、小包配達書への署名等である。

したがって、署名は、例えば、遠隔地にあるコンピュータシステムにアクセスを許可する前にその確認のために遠隔地に送ることができる。また、署名は特定

の人が特定の文書または処理を許可したことの記録としてコンピュータのアーカイブ（保管所：Archive）

に記憶される。また、使用者に特定の電子文書へのアクセスを許可してよいかどうかを即座に決定するために署名を確認することが望ましい。

本発明は署名データ（特に署名エンベロープ）が詐欺的誤用を受けることを許さない。したがって、クライアント・プログラムは、コード化形式のものを除く署名データへのアクセスを行うことはできないし、また偽造に対し実質的に助けとなると思われる情報を得ることはできない。

本発明の独特な安全性は以下の点にある。即ち、本発明では、生の署名データを署名確認装置に伝送するのではなく（即ち、署名採取モジュールが生の署名データを署名確認モジュールに伝送するのではなく）、署名採取の段階で署名の特色抽出が行われる。代表的な実施例では、生の署名データは署名エンベロープに記憶されず、また如何なる段階に置いてもクライアント・プログラムが利用できないようにしてある。したがって、署名エンベロープを調べて生の署名データを改造し、その後でその生の署名データをシステムに再度挿入することができないようにしてある。また、このことは署名確認前に伝送または保管される情報量を削減する。

本発明は電子文書の不法修正の検出補助に利用できる。上記したように、文書の検査合計値は文書を形成している文字コードから計算され、署名エンベロープの一部としてその文書とは別に記憶される。修正文書から得られる文書の検査合計値は元のものとは違うから、その修正を検出することができる。本発明は、インクが紙上で乾くことに対する完全な電子的比喩を支持して、進歩した検査合計方法を用いて署名エンベロープを文書に結びつける。このことは、重要プロンプトと共に、一文書に対してなされた署名が他の文書に使用されないように、一署名一意使用の維持を支援するものである。

図面の簡単な説明

図１は本発明による典型的なシステム構造を示すブロック図である。

図２は第１のプラットフォームで採取された署名を、第２のプラットフォームで確認する場合に使用するような本発明による典型的なシステム構造を示すブロック図である。

図３は手書き署名の採取に使用するウインドウおよび重要プロンプトの例を示す図である。

図３Ａは他の重要プロンプトの例を示す図である。

図４は署名エンベロープのライフサイクルを示す流れ図である。

図５は署名採取過程の典型的段階を示す流れ図である。

図６は本発明によるテンプレート・ソフトウェアオブジェクトに関する典型的なライフサイクルを示す流れ図である。

図７はテンプレート登録過程の典型的な段階を示す流れ図である。

図８は本発明のエンティティ（Entity）に関するエンティティ関係図である。

図９は人物を表すソフトウェアオブジェクトのライフサイクルを示す図である。

詳細な説明

図面参照にて、図１には本発明の構成要素を利用した典型的なシステムがブロック図形式で示されている。

第１図は署名の採取と確認の機能が同一装置で実行される構成を示すものである。クライアント・アプリケーション２は署名の採取を要求する。このクライアント・アプリケーションはこの要求情報

を署名採取モジュール４（署名採取サービスとも呼ばれる）に提示し、そしてこの署名採取モジュールはユーザーが彼のまたは彼女の署名を適当なハードウエア装置、例えば、ペン／ディジタイザとデイスプレイ６との組合せを使用して署名することを要求する。この署名採取モジュール４は、後述するような、署名エンベロープ１０を作成してこれをクライアント・アプリケーション２に渡す（または使用できるようにする）。

クライアント・アプリケーション２が署名の確認を望むときには、これはその署名エンベロープ１０を署名確認モジュール６（署名確認サービスともいわれる

）に渡す。署名確認モジュール６は、その署名の署名情報とその署名の“所有者”に関する情報のテンプレートを内容とするテンプレート・データベース１２（署名者データベースとも呼ばれる）にアクセスし、そして署名対応率をクライアント・アプリケーション２に戻す。

図２は、署名がペン装備のコンピュータで採取されるが、遠隔システムにて確認される構成を示すものである。図２においては、２つのクライアント・アプリケーション２aおよび２bがある。この実施例においては、クライアント・アプリケーション２aはペン装備コンピュータに搭載されている。署名採取モジュール４は署名を採取して署名エンベロープ１０をクライアント・アプリケーション２aに戻す。この署名エンベロープ１０は別のクライアント・アプリケーション、例えば、クライアント・アプリケーション２ｂに送ることができる。クライアント・アプリケーション２ｂは、署名エンベロープ１０により提示される署名が確認されることを要求することができる。この場合には、クライアント・アプリケーション２aはその署名エンベロープ１０を署名確認モジュール６に渡し、この署名確認モジュール６が上記署名を確認する。

本発明のこのオープン構成は多くの変更形態を可能とすることが注目される。例えば、この署名確認モジュール６とテンプレート・データベース１２を単一のコンピュータシステムに搭載することができる。また、多数の署名確認モジュール６を相異なるプラットフォームに搭載して、その全てが遠隔配置された１つのテンプレート・データベース１２にアクセスできるようにすることができる。

この署名採取モジュール４と署名確認モジュール６は１組のＡＰＩ(アプリケーション・プログラム・インタフェース)を利用して署名の採取および確認を多数の相異なるアプリケーション、例えば、２a、２bに組込むことを可能としている。アプリケーションは各署名の背景や署名確認の識閾（Criteria）を決定することができる。

この代表的な実施例においては、本発明はＩＢＭ社（International Business Machines Corp.）のＯＳ／２（Ｃ＋＋インタフェース）用のペンおよびマイクロソフト社(Microsoft Corp.)のペン計算〔Ｃ＋＋およびビジュアル・ベーシッ

ク・インタフェース（Visual Basic Interface）］用ウインドウズにおいて実施される。署名採取モジュール４および署名確認モジュール６は別のコンピュータプログラムに組込まれるか、あるいは別のコンピュータプログラムにより作動されるように指定されている。したがって、これらは自給式ソフトウエア構成要素と考えるべきである。

この代表的な実施例においては、署名採取モジュール４は図式デイスプレイ装置およびディジタイザの両者の利用性を要件とする。ペン計算およびＯＳ／２用のペン用の両ウインドウのもとでは、その動作システムにより支援される図式デイスプレイ装置はいかなるものも使用され得る。例えば、ワコム(Wacom)、カルコンプ(Calcomp)、クルタ(Kuruta)等が使用可能である。加えて、このコンピュー・プロセッサは、例えば、コンパック(Compaq)のコンサート

・コンピュータ（Concerto Computer）またはＩＢＭのＰシリーズ・シンクパッド・コンピュータ（P.Series Thinkpad Computer）のような動作システムのいずれか一方を支援するペンベースのコンピュータとすることができる。

署名確認モジュール６は、特定のハードウエアを要件とせず、この代表的な実施例においては、Ｃ＋＋コンパイラまたはクロス・コンパイラを支援するコンピュータ動作システムのもとで実施することができる。

本発明は次の３つの分離可能なサブシステムを持つと考えることができる。即ち、

１．署名採取モジュール４；これは署名エンベロープ１０に署名して同署名エンベロープを作成する行為を記録する。

２．署名確認モジュール６；これは個人の署名プロフィル、即ち、“テンプレート”に基いて署名エンベロープを測定する。

３．テンプレート・データベース１２。

これらの３つのサブシステムの用途を示すためには、コンピュータシステムへのアクセスを統制すべく署名確認の単純な適用を考慮することが必要である。この場合のクライアント・プログラム２は署名の採取を要望し、ついで、これを確認してコンピュータ・ユーザーの身元に関する証拠を受取る。この場合、そのス

テップは次の通りである：

＊　ユーザーが主張する身元を確定する。

＊　ユーザーの署名をその日時と共に採取する。

＊　ユーザーが主張する身元を使用してその署名テンプレートの場所を確定する。

＊　その署名がそのユーザーのテンプレートに対応しているか否かを確定する。

これらのステップは、上記３つのサブシステムとの関係において次のように説明することができる：

＊　ユーザーが主張する身元を確定した後、そのユーザーの識別子を有する空のエンベロープを作成する。

＊　署名採取モジュール４をして署名データを収集させて、その日時と署名の理由の文字通りの表現と共に署名エンベロープに入れる。

＊　署名確認モジュール６をしてテンプレート・データベース１２をサーチさせ、署名エンベロープ１０に保存されているその署名者のテンプレートの場所を確定させる。

＊　署名確認モジュール６をして、その署名エンベロープ１０が見出されたテンプレートに基いて確認させる。

署名確認モジュール６は、この代表的な実施例においては次のように動作する。各署名の測定（署名エンベロープ１０から得られたもの）とその平均（そのテンプレートから得られたもの）との差が計算され、そして記載時に計算される測定のための標準偏差により割算される。その最高結果値が保存され、そして全ての値が総計されて平均化される。最高値と平均値は２つの係数により算定されて比較可能値となし、このうちの最大のものが保持される。もしこれが所定の（小さい）値Ｍよりも小さければ、最大得点１００が戻される。同様にして、もしこれが所定の（大きい）値よりも大きければ、最小得点が戻される。別の手法としては、この結果値をＭ＋１から除算し、その差を１００で乗算して０から１００までの範囲の値を出す。ついで、この値がクライアント・アプリケーション２に

戻される。

得点をクライアント・アプリケーション２に戻すことは、クライアント・アプリケーション２が特定の処理との関係においてその署

名が合格か落第かを決定できるようにする。例えば、署名されている文書が＄１，０００（１，０００ドル）のローン文書であれば、合格点として得点７５またはこれ以上の得点がクライアント・アプリケーション２により要求される。しかし、署名されている文書が銀行口座から＄２００，０００を下ろすための下ろし伝票であれば、この場合は、クライアント・アプリケーション２は合格点として得点９５またはこれ以上の得点を要求することができる。

この構成を使用して、本発明は手書きの署名の採取と確認が相異なるプラットフォーム上で行えるようにすることができる。本発明は輸送可能なデータ式記録、署名の行為を記録するタイプの輸送可能なデータを創作し、そしてこれが文書とリンク（または“結合”）できるようにする。

本発明は、それぞれにおいて動作が実行されて機構が相互作用を可能とする３つのサブシステムの性質を参照することにより最もよく理解することができる。

１．署名エンベロープ１０

署名エンベロープ１０は、署名の物理的行為をディジタル記録するコード化データの複雑な包みとして考えることができる。

しかし、署名の行為は純粋には物理的行為とは考えられない。実際には、このような行為は、署名人の意図、日時、および署名される文書等の一連の関係から分離することはできない。署名エンベロープ１０は、これら本質的な付随要素に関するデータもその内容とする。

署名が採取されるに先立ち、署名採取モジュール４は、通常はクライアント・アプリケーション２から、次の情報が与えられる：

＊　署名に際してのユーザーの意図の要旨（短いテキストの形

式）；これは署名採取モジュール４により、ユーザーの署名が表示されるコンピュータのデイスプレイの領域に近接して目立つ状態で表示される。この短いテキ

ストは「重要プロンプト」として知られている。これは署名の行為の重量（重要性）を知らせるからである。例えば、重要プロンプトでは、“私はジョージ　ビール（George Beals）に＄４９．５０支払うことに同意する”、または“私は私の家をフレッド　デニング（Fred Denning）に＄２３，０００で売ることに同意する”、または“あなたは「手紙」という名称の文書に署名しています、ファイル名はlet.wp”、または“クレジット契約書に同意の署名をして下さい”と書くことができる。

＊　任意ではあるが、ユーザーが署名する文書を示すコンピュータ・ファイルの参照。

＊　任意ではあるが、署名の可視表示が署名エンベロープ１０の内側に保存されるべきか否か。

＊　任意ではあるが、保全のための検査合計値の生成にキーを使用するか否か。

署名採取プロセスが開始すると、用紙またはウインドウ２０（図３に示す）がコンピュータのスクリーンに表示され、そして重要プロンプト２２が署名採取モジュール４により表示される（図３において、重要プロンプトには“登録が不完全ー登録のための署名をして下さい”と書かれている。この重要プロンプトは、以下に詳しく説明するが、テンプレート作成時の登録プロセスにおいて使用され、ユーザーに彼がテンプレート作成のための署名をしていることを知らせる）。ユーザーはいつでも用紙上に表示の“取消し”制御部２４を作動させることで、即ち、これを彼のペンでたたくことでその処理の取消しを選択することができる。

ユーザーはまた、“クリア”制御部２６を同様に作動させること

により署名の採取（例えば、腕を揺することによって）を再度開始することもできる。ユーザーが“ＯＫ”制御部２８を作動させれば署名の採取は完了するが、これは次の仕様に基くものである：

＊　署名は完了まで一定の時間を要するものでなければならない。

＊　引く線の長さは一定の最小限度よりも長くなくてはならない。

＊　署名データは一定の複雑さを提示するものでなければならない。

＊　ペンは２秒以上静止してはならない。

これら仕様のいずれかに違反した場合には、署名者にメッセージが表示されてその署名は拒絶され（ユーザーが“クリア”制御部２６を操作したと同様）、システムは自動的に別の署名を受入れる状態となる。

この時点で署名採取モジュール４は署名エンベロープ１０に次の情報を保存する：

＊　署名の行為の日時。

＊　重要プロンプト。

＊　署名人が主張する身元。

＊　署名が採取された機器の身元。

＊　署名の採取を開始したコンピュータ・プログラムを代表する確認者、即ち、クライアント・アプリケーション２。

＊　署名に関する測定および統計、例えば、形、ペンの筆跡、署名に要した全時間等。

＊　任意ではあるが、採取された署名が関係するファイルまたは文書として、照合が最初に指定されたコンピュータ・ファイルまたは文書メントから計算される検査合計値(checksum)。

＊　任意ではあるが、署名のイメージをベクトル形式で圧縮した表示。

＊　保全のための検査合計値(checksum)。

本発明は署名採取後の署名エンベロープ１０の変更を許可しない。署名エンベロープ１０に保持されたデータはコード化に先だって合計チエックが為されて，未公認の修正が検知できるようになっている。

図３Ａに示すように、クライアント・アプリケーション２は署名採取モジュール４に、署名されている文書の身元および、またはその文書が署名されている理由（または重要性）を供給することができる。この情報が重要プロンプト２２である。この代表的な実施例においては、重要プロンプト２２は署名採取ウインドウ２０においてユーザーに表示されている。これによってユーザーは、署名して

いる文書は彼または彼女がいまこれに署名しているのだと信じる文書であることを確認することができ、更に署名の行為のグラビテイ（重み）の理由を認識することができる。この代表的な実施例においては、重要プロンプト２２は署名エンベロープ１０に保存される。したがって、この重要プロンプト２２は後の段階で別のアプリケーション（これらは別のプラットフォームで操作することができる）により回復されて表示することができる。図３Ａに示すように、署名されている文書は全５頁の消費者クレジット・アプリケーションであり、その一部がウインドウ３０に表示されている。署名されている文書のタイトルは文書用のタイトル・バー３２においてクライアント・アプリケーション２により表示される。重要プロンプト２２には、“クレジット契約書（合意書）承認の署名をして下さい”と書かれている。このテキスト“クレジット契約書承認の署名をして下さい”は、クライアント・アプリケーション２が署名採取モジュール４に供給したものであり、このテキストは署名エンベロープ

１０に保存される。署名採取ウインドウ２０は、図３Ａにおいて、署名されている文書を内容とするウインドウ３０に表示されている。

本発明（この代表的な実施例においては、署名確認モジュール６は下記の機能を実行する）は、クライアント・アプリケーション２の要求がある場合、署名エンベロープ１０に関連して次の機能を提供する：

＊　署名人が主張する身元の開示。

＊　署名の行為の日時の開示。

＊　署名が採取されたときに文書の合計データの検査の選択が実行された場合に、文書を代表する所定のコンピュータ・ファイルが、最初に検査合計値のチエックがなされたものと同一か否かの確認。

＊　署名が採取された場合、その署名の可視表示の保存の選択が実行されたときに、その署名をコンピュータのスクリーンに表示できること。

＊　署名が採取された場合、その署名の可視表示の保存の選択が実行されたときに、その可視表示を内容とする標準フォーマットのデイスク・ファイルをビット・マップ形式で生成できること。

＊　テンプレートに基く確認。

加えて、本発明は、署名エンベロープ１０に関連して次の機能を実行することができる：

＊　保管、または遠隔システムへの送信を可能とするために、メモリからデータ・ブロックへのコード化。

＊　アーカイブ（保管所）から、または電子的データ送信を介して回復されたデータ・ブロックからメモリにおける署名エンベロープ１０の作成。

メモリから回復されるデータ・ブロックは最初に書出されたオブジェクトと同一のオブジェクトを再構成するに足るデータを内容と

する暗号ブロックのメモリである。データ・ブロックは、オリジナル・オブジェクトの全状態を保存し、且つ同じまたは遠隔システムで再生できるようにするプロック情報であって、効果的にコード化され、そしてポータブルのものである。

これらのデータ・ブロックは、オブジェクトを保管所に保管するために、あるいはオブジェクトのコピーを遠隔システムに送信するために使用される。本質的にはこれらデータ・ブロックはオリジナル・オブジェクトと同じ情報を内容とするが、このデータ・オブジェクトが後日同じデータ・ブロックから再構成できるように高度に構築された形式で表現される。

この代表的な実施例においては、署名エンベロープ１０はソフトウエアオブジェクトとして圧縮される。典型的な署名エンベロープのソフトウエアオブジェクトの表示は次の通りである：

データ

署名エンベロープの版番号

機器の連続番号

機器のブート時間

機器のタイプ（番号）

主張された身元（採取アプリケーションにより認識された署名者を確認する一連の文字）

ヘッダ・テキスト（可変長さのＡＳＣＩＩテキスト）

署名人の外観ファイル検査合計値の圧縮表示

キーが施された保全用の内部検査合計値

方法

採取する　：UI構成要素を表示し、署名を収集する

表示する　：採取した署名のイメージをデイスプレイ上に描く

tiffファイルに書込む　：イメージをTIFFフォーマット・ファイルに書込む

win bmpファイルに書込む　：ウインドウ・ビットマップ・フォーマットに書込む

os2 bmpファイルに書き込む　：ＯＳ／２ビットマップ・フォーマット・ファイルに書込む

採取される　：署名エンベロープ１０が署名を内容とするか否かを報告する

イメージを持つ　：署名エンベロープ１０がイメージを内容とするか否かを報告する

機器の連続番号　：採取機器の連続番号を報告する

機器のタイプ　：採取機器のタイプを報告する

署名時　：採取の日時を報告する

主張される身元　：主張される身元の素線を報告する

重要プロンプト　：重要プロンプトを報告する

ファイルを確認する　：保存された検査合計値に基いてファイルの内容をチエックする

移入する（Import）　：コード化されたデータ・ブロックからデータを書込む

移出する（Export）　：コード化された内部データでデータ・ブロックを書込む

本発明の署名エンベロープ・オブジェクトの典型的なライフサイ

クルは図４にフロー・チャート形式で要約されており、これを以下詳細に説明する。

生成（ステップ１００）

ソフトウエアオブジェクトが生成される時には、これは署名の採取が開始される状態に初期化される。

採取／移入

採取（ステップ１０２）

採取プロセスにおけるイベント（Event）のシーケンスは図５にさらに詳しく示されている。採取ステップ（１０２）は、この代表的な実施例においては、署名採取モジュール４により実行される。

署名エンベロープ１０のオブジェクトが前もって採取された場合には、採取の要求は否定される。

クライアント・プログラムは、重要プロンプトが表示されるべく、署名イメージが保持さるべきか否か、および、文書綴じのために文書の検査合計値のチェックがなされるべきか否かを指定する。

文書の検査合計値のチェックがなされる場合には、その文書が保存されているファイルが熟読されて検査合計値が確立される。本発明の代表的な実施例はＲＳＡ社により公開されているような文書の検査合計値チェックのためのメッセージ・ダイジェスト技術を使用する。

ついで、ユーザー・インタフェース構成要素がコンピュータのグラフィック・スクリーンに顕著な状態で表示され、確実かつ拘束力ある署名が採取されねばならないという事実に注意を喚起する（例えば、図１参照）。

ユーザーが“取消し”制御部２４を操作した場合には、適切なる

状態がクライアント・プログラムに戻される（ステップ２０２および２０４）。

ユーザーが“クリア”制御部２６を操作した場合には（ステップ２０６）、先に収集されたペン・データが破棄されて放棄された署名はデイスプレイからクリアされる（ステップ２０８）。

ユーザーがペンを署名採取領域で操作すると（ステップ２１０）、ペンの動き

を表すデータが収集されてメモリに保存される（ステップ２１２）。ユーザーが“ＯＫ”制御部を操作すると（ステップ２１４）、署名採取モジュール４が採取したペン・データを分析して特定の測定を記録する。この代表的な実施例においては、署名採取モジュール４が実行する測定は次の通りである：

ＭＯ	ストローク数
Ｍ１	全時間
Ｍ２	ペンが下っている時間
Ｍ２３	線の全長
Ｍ２３／ＭＯ	平均ストローク長さ
Ｍ２／ＭＯ	ペンが下っている時間／ストローク数
Ｍ１／Ｍ２３	平均速度
	各ストロークにおける最低速度点の時間の総計
	各ストロークにおける最高速度点の時間の総計
Ｍ３４	各ストロークにおける最低速度点の位置の総数
Ｍ３５	各ストロークにおける最高速度点の位置の総数
Ｍ３６	ペンが下っている位置の総数
Ｍ３７	ペンが上っている位置の総数
Ｍ３８	加速および減速の最大（「イベント」）の数
Ｍ４０	イベント位置の総数
Ｍ４１	イベント時間の総計
	ペンが下がっている時の平均時間
	ペンが上がっている時の平均時間
Ｍ３５／Ｍ１	最高速度点の時間のねじれ
Ｍ３７／Ｍ２３	ペンが上がっている位置の縮尺総数
Ｍ２３／Ｍ３８	平均加速／減速
	距離
Ｍ３９／Ｍ２３	イベントの期間の総計／線の全長
Ｍ４０／Ｍ１	イベント時間のねじれ

Ｍ４１／Ｍ３８　イベントの平均時間

－ve／＋vdのＹ方向距離

＋ve／－veのＸ方向距離

Ｙ方向距離／Ｘ方向距離

最大Ｘ／最大Ｙ

Ｙ方向距離／（最大Ｙ＋１）

Ｙ方向転向の数、幅＞０．８mm

純領域

速度デルタの差の総数

任意ではあるが、ペン・データは時間情報なくして圧縮され、ベクトル化されて、コンピュータ・デイスプレイ・スクリーンまたはビットマップ・ファイルへの署名のイメージとするために保存される。署名の日時、機器の詳細および重要プロンプトも同様に保存さ

れる。ついで、データブロックの検査合計値が生成されてその後の変更を防止する（ステップ２１６）。

本発明は内蔵の保全チェックを含み、これは次のように説明することができる。コード化に先だって、署名エンベロープ１０の内容は、クライアント・アプリケーション２により提供されるキーと共に、ファイルの検査合計に使用したのと同じ技術で検査合計値がチェックされる。したがって、署名エンベロープ１０を構築させたときのオリジナル・クライアント・アプリケーション２が使用するキーを知らずして署名エンベロープ１０を修正して満足のゆく検査合計値を再生成することは不可能である。保全のチェックを実行するときにこの訂正キーを提供することでクライアント・アプリケーション２は（このキーが開示されていなかった限り）署名エンベロープ１０は解読、修正および再コード化がなされなかったことを保証することができる（ステップ１０４）。

先に採取された署名データはメモリ・ブロックから解読されてデータ構成に適切に保存される。

データアクセス（ステップ１０６）

本実施の形態において、データアクセス機能は署名確認モジュール６によって行われる。

移出（エクスポート）

署名エンベロープ１０内のデータは、メモリ・ブロックに記憶され、コード化される。

署名画像（署名イメージ）をコンピュータ・ディスプレイ上で表示すること（Render）

署名イメージが、本来エンベロープを採取したクライアント・プログラム２によって要求されなければ、表示を要求するクライアン

トはエラー状態に戻る。

クライアント・プログラム２が署名イメージを要求すれば、署名イメージは適当な寸法で表示される。

ビットマップ・ファイルの作成

ビットマップ・ファイルは、標準的なイメージファイル・フォーマットを用いて作成される。本発明の実施の形態に用いられるフォーマットとして、以下に示すフォーマットが推奨される。

ＴＩＦＦ

ＯＳ／２ビットマップ

ウィンドウズ（Ｗｉｎｄｏｗｓ）・ビットマップ

クライアント・プログラムからの要求に応じて、本発明のシステムは、以下の事項に関する復号情報をクライアント・プログラムがアクセスできるメモリに配置する。

要求ＩＤ（アイデンティティ：Identity）

署名の日時

移出されたデータ・ブロックのサイズ

署名エンベロープ１０が採取署名を含むか否か

署名エンベロープ１０が署名イメージを含むか否か

署名が採取された機器のシリアル番号

署名が採取された機器の型を示す番号

重要プロンプト

内蔵保護チェックが成功したか失敗したか

署名を採取したとき、付与されたファイルが元々チェック済みと判断されたファイルと一致するか否か

破壊（ステップ１０８）

依存データの割当ては、破壊される。

２．テンプレート

テンプレートは、クライアント・プログラム２によって直接扱えないが、その代わり、テンプレートのデータベースを実施するソフトウェアの構成要素の媒体を介してアクセスされる。

まず、テンプレートが作成されると、テンプレートはブランクである。本発明によって、クライアント・プログラム２はテンプレートを検知し、連続する署名エンベロープ１０を用いてテンプレートを“満たす”ことができる。このプロセスは、“登録”として知られているように、一般的な署名実行者の動作および署名実行者の動作が最適に首尾一貫していることが決定される間の学習プロセスに相当する。

登録段階の間、受け取られた署名エンベロープ１０同士がどの程度類似しているかが、最終的なテンプレートの質に影響する。署名エンベロープが全く異なる場合、確認は不可能になり、登録プロセスは始めからやり直される。署名エンベロープが同じ場合、登録の間に受け取られた署名エンベロープがどの程度一致しているかが、確認スコアを考慮して確められる。一致の程度が高いほど、確認プロセスの信頼性は高くなる。

テンプレートが完全であることは、セキュリティを意識したアプリケーション・プログラムにとって非常に重要なので、テンプレートは“所有”アプリケーションに関する情報を含む。テンプレートの所有者のみが、その情報に対して敏感に対応して操作を行うことができる。

テンプレートは、以下の情報を記憶している。

・署名計測値と統計値との平均値

・これらの統計値の可変量の表示

・登録の状態および質の表示

・署名エンベロープ１０が一番最近に確認された日時

・パフォーマンス表示

・“所有”プログラムのＩＤ

・作成日時

・独自の識別子

本発明は、テンプレートに関連する以下の機能を提供する。

・作成日時の開示

・登録の状態および質の開示

・署名エンベロープ１０の登録（所有プログラムのみ）

・強制再登録（所有プログラムのみ）

・署名エンベロープ１０の確認

確認手順は、クライアント・プログラム２にスコアフォームで偽の署名である可能性を示すのに役立つ。このスコアは、多くの場合登録の質に関する情報とともに、クライアント・プログラムがその判断基準に基づいて署名を許可できるかどうかを決定させることができる。

時間がたつにつれて個々の署名が徐々に変化するので、本発明は、ある環境において、署名動作が一貫して変化するように署名エンベロープ１０を“ベンディング（Bending）する”。この「ベンディング」とは、ある内部チェックに基づいて行われ、クライアント・アプリケーションによって選択的に抑制できる。確認される署名エンベロープ１０が、ひき続いて確認される最新の署名エンベロープ

よりも古い場合、再び「ベンディング」は行われない（図６のステップ３１８を参照、詳細は以下に示す）。

本発明の本実施の形態において、各テンプレートはソフトウェアのオブジェク

トとして実行される。テンプレートのソフトウェアオブジェクトの一般的なライフサイクルの概要は、図６のフローチャートに示され、詳細は以下に記載される。

作成（ステップ３０２）

テンプレートのソフトウェアオブジェクトが作成されると、登録、移入（インポート）または移出が初期化できる状態に初期化される。

登録（ステップ３１０）

本発明は、テンプレートが非登録状態にある場合のみ、テンプレート登録ができる。　登録プロセスの概要は、図７のフローチャートに示される。

署名の所定の最小値は、本発明のシステムが登録を終了させようとする前に、提示されなければならない。この時点に到達するまでは、連続する署名エンベロープ１０からのデータは、不完全なテンプレートとともに記憶されるだけである（ステップ４０２）。

いったん署名エンベロープの最小番号が受け取られると（ステップ４０６）、本発明はチェックを行い、提示された署名エンベロープがテンプレートを作成するのに十分一貫しているかどうかを決定する。もし、十分一貫していなければ、すべての署名エンベロープは消去（クリア）され、テンプレートは初期状態に再設定される（ステップ４１４および４２０）。他方、もし提示された署名エンベロープが十分一貫していれば、テンプレート統計値が発生し（ステップ４０８）、記憶された署名エンベロープは不要になり、テン

プレートは登録完了のマークが付けられる。

しかしながら、署名エンベロープの最小番号が受け取られ、テンプレートの改良が許可されると（ステップ４１６）、さらに所定の最大値までの署名エンベロープが受け入れられる。もっとも一致する設定は、良好な登録が確立できるまでまたは最大値に達成するまで保持され、どちらが早くてもよい。

移入（ステップ３０４）

予めコンパイルされたテンプレートデータは、メモリ・ブロックから復号され、データ構造に適切に記憶される。

移出（ステップ３２０）

テンプレートデータは、リモートシステムに到達または伝送されるためにメモリ・ブロックでコード化される。

確認（ステップ３１４）

署名確認モジュール６は、テンプレートが登録状態のときのみ、テンプレートに対する署名エンベロープ１０の確認が行われる。

署名採取プロセスの間に計測され、署名エンベロープ１０に記憶された計測値は、テンプレートに記憶された中間値と比較される。登録プロセスの間監視が行われながら、ユーザーの可変量がカウントされる。２つの数値が発生し、１つは、中間値からの平均エラーを示し、もう１つは中間値からの最大の分散値を示す。それから、これら２つの値の機能が用いられ、０．．．１００の範囲でスコアが作成される。ここで、０は署名エンベロープとエンベロープの不一致を示し、１００は署名エンベロープとエンベロープの一致を示

す。署名確認モジュール６のこの特徴の詳細については、前述のとおりである。

クライアント・アプリケーションが確認のための署名エンベロープ１０を提供するとき、テンプレート更新のための低しきい値として作用するスコア値も提供する。テンプレートの更新（または「ベンディング」）（ステップ３１８を参照）は、以下の条件を前提として行われる。

・確認スコアは、しきい値以上の値である。

・確認値は、中間値に近すぎることなく、遠すぎることもない値である。

・署名エンベロープ１０は、以前に確認された署名エンベロープ１０より最近のものである。

・確認スコアは、クライアント・プログラム２によって提供されたしきい値より高い値である。

以上の条件を満たせば（ステップ３１６）、テンプレート内に記憶された中間値が訂正され、ある時間にわたって、テンプレートはテンプレート署名実行者の操作の流れに順応する。更新が行われると、テンプレートにタイムスタンプが行われ、複数または遠隔のテンプレートのコピーの管理が容易に行われる。

消去（ステップ３１２）

本発明によれば、テンプレートを再登録可能な状態にできる。作成日時は保持され、テンプレートの更新日時は、登録状態においてデータアクセスの現日時に設定される（ステップ３０６）。テンプレートが登録されたかどうかの調査に応じて、システムは情報のブロックを終了させる（以下に示す）。これはクライアント・プログラム２による調査に利用できる。

本実施の形態において、情報のブロックは、以下のような構成である。

・update_time　統計値が最近更新された時間
・backup_time　テンプレートが最近バックアップされた時間
・count　登録を終了させるために用いられた署名の番号
・enroll_state　登録の一致を示す番号
・enroll_flag　登録が完了すると、非ゼロ値を示す

３．テンプレート・データベース１２

署名テンプレートは、個々独自のものである。いったんテンプレートが構成されると、そのテンプレートを用いて個人を確認し、ユーザーが本発明のシステムを用いて署名した文書が本物であると認める。明らかに、個々の署名は、１つ以上のクライアント・プログラム２または１つ以上の構成に関連する。テンプレートデータベース１２は、１つ以上のアプリケーション２に利用できるように設計されている。このため、確認をする目的で、所有テンプレートまたは登録テンプレートを他のクライアントに用いることによって、テンプレートの“所有者”は、所有テンプレートまたは登録テンプレートから商業的な利益を得る。

テンプレートデータベース１２のデータベース構築は、以下の目的に基づく。

・データベースサービスを利用する前に、クライアント・アプリケーション２は、システムによって作成された特定の識別子を用いて本発明のシステムに確認されなければならない。特定の識別子は、あるアプリケーションが本発明のシステムに登録されるとき、作成される。クライアント・アプリケーションがテンプレートを作成す

る前に、登録を行う必要がある。

・テンプレートが作成される場合、個人名およびユーザー独自の確認番号（例えば、国民健康保険番号または社会保険番号）を含むデータベース記録も作成され、以下、修正できない。この記録を用いて、クライアント・アプリケーションの様々な識別子を同一個人に一致させる。

・本発明のシステムは、合致データのいかなる組み合わせに対してテンプレートデータベース１２をサーチし、あるテンプレートと合致すると関連づける。

・テンプレートを作成する場合または特定のサーチパターンに合致する場合において、本発明のシステムは、クライアント・アプリケーション２に個々のアプリケーション独自の識別子を登録する能力が付与される。以下、クライアントは、好適な識別子を提供しさえすればよい。これは、クライアント・プログラム２が常に署名が確認される個人に関連する独自の識別子のインデックスを有することを認識する。

・クライアントのインストールが適正な使用許諾権を有する場合、本発明のシステムは、別に記録したり伝送するために、テンプレートの記録を、コード化されたデータ・ブロックに変換する。

本発明の構造は、署名確認部の新しい概念に役立ち、いかなる数のクライアント２に対しても遠隔またはネットワークでの確認サービスを提供する。

本発明のシステムは、署名テンプレートのリモートメンテナンスまたはリモート管理にも役立つ。これは、中央部に構築されたテンプレートが中央データベースから独立して“オフライン”確認を行うリモートプロセッサに分配される必要がある場合、非常に重要で

ある。その例として、スマートカード、または小型携帯ペン操作式コンピュータの“フリート（Fleet）”の利用を含み、ここで署名テンプレートの中央集中記憶装置は、正確なセキュリティ構成を用いてフィールド内の装置の欠陥処理およびその欠陥の迅速な交換を行うために重要である。

テンプレート・データベース１２の目的は、アプリケーション・プログラム（例えば、２b）が必要とする全てのテンプレートを記憶することである。しかし

ながら、テンプレート・データベース１２特有の構造は、それぞれ異なるアプリケーションが１つのテンプレートを共用できるように、個別のテンプレートを１つ以上のアプリケーションに利用させることである。

これは、データベース機能が利用できるようになる前に、強制的にクライアント・アプリケーション２がデータベースセッションを開始させることによって、達成される。セッションが開始されると、クライアント・アプリケーション２は、その確認を明らかにしなければならない。

データベース１２は、独自の確認情報とともにテンプレートを示すために個人の概念を用いる。データベース１２内に記憶された全てのテンプレートは各人に属し、どの個人もアプリケーションのいずれかに登録される。いずれか１つのアプリケーションはそのアプリケーションに登録された個人を多数有し、いずれか１人の個人はアプリケーションのいくつかに登録される。これは、図８のエンティティ関係図に示される。

まず、他のデータベースサービスが利用できるようになる前に、クライアント・アプリケーション２はシステムに認知されなければならない。アプリケーション２がセッション（Session）を開始すると、アプリケーション２は他のすべてのアプリケーションに認知

されることによって、アプリケーション２自身を表すパブリックネームを明らかにする。アプリケーション２は、シークレット暗号キーも提供する。このキーは本発明によって用いられ、ＡＩＤとして知られるアプリケーションの独自ＩＤを作成する。同時に、テンプレートにアクセスするとき、個人を確認するために用いられる独自の識別子の長さに関する情報も提供する。クライアント・アプリケーション２がテンプレートを作成することを必要とする場合、まず他のアプリケーションに既に登録されている個人のデータベース１２を走査する。ある個人が登録されると、テンプレートが作成され、他の情報（氏名、ユーザーＩＤ番号）も記憶される。このため、これらの判断基準用いるアプリケーションは、当該個人がクライアント・アプリケーション２に既に登録されているか否かを決定できる。

もし合致する個人が見つからなければ、新しい個人データが作成され、データベース１２に追加される。

本実施の形態において、個人はソフトウェアのオブジェクトによって示される。この個人に関するソフトウェアオブジェクトのライフサイクルは、図９に示される。データベース１２は、個人のオブジェクト操作を介してクライアント・アプリケーション２の代わりにすべてのテンプレート操作を行う。

ある個人は、その個人に対応するテンプレートとともに、テンプレートを作成するアプリケーション２によって“所有されている”とみなされる。テンプレートの登録およびクリアを含むテンプレートに対する操作は、所有アプリケーション２によってのみ行われる。しかしながら、所有アプリケーションは、他のアプリケーションがテンプレートのロック解除のために用いるパスワードを特定することによって、登録を他のアプリケーションに利用する。

ある個人に関連する名前および独自のユーザーＩＤ番号を独自に

用い、全てのアプリケーションにわたってその個人を確認する。その結果、これらのデータは不変である。

個人をアプリケーションに登録する

いったんある個人データがアプリケーション２によって作成され、配置されると、アプリケーション２はその個人をアプリケーション２そのものに登録できる。これは、アプリケーションの独自の個人識別子（一般的に、その個人を確認するためアプリケーションによって用いられる独自のキー）を供給することによって、達成される。独自のキーの長さは、そのキーがまずデータベース１２に登録されたとき、アプリケーション２によって明らかにされる。この識別子は、アプリケーション独自の識別子（ＡＵＩＤ）として知られ、以下、このＡＵＩＤは、個人またはその個人のテンプレートを確認するためのアプリケーションによって用いられる。

登録の際、本発明はＡＵＩＤを含む新しいデータベース記録を構成し、アプリケーションを用いて、新しい記録と以前に記録された登録とをリンクさせたり、他のアプリケーションを用いて、新しい記録とその個人に関する以前の登録とを

リンクさせる。

アプリケーションは、以下に関するデータベースを走査する。

・全てのアプリケーション

・アプリケーションに登録された全ての個人

・アプリケーションに登録されていない全ての個人

・合致判断基準に合う全ての人

本発明は、図６のステップ３１０に示すように、時間が経過するにつれて、個々の署名テンプレートをユーザーの署名の変化に応じて“修正する”。例えば、署名実行者が２秒前後で自分の名前を署

名する。これは、およそ１／１０秒の範囲で変化し、署名確認モジュール６は、署名実行者の署名に要する時間が２．２秒または１．９秒続くと、“その署名実行者をマーク”しない（すなわち、その署名実行者の署名合致の割合を低下させない）。しかし、数ヶ月後（大抵、ユーザーが用いる装置に慣れていない場合）、ユーザーの署名は、１．９秒でマークされる傾向にある。他の全てのデータが署名実行者の登録に対してほぼ適正なので、署名確認モジュール６は、署名実行者の署名テンプレートをわずかに“ベンド”し、署名実行者の署名操作のパターンまたは変更に従う。１年後、署名実行者は１．８秒でまちがいなく署名するが、１．７秒または１．９秒かかる場合もある。この時間によって、中間値は署名実行者の操作に従い、１．８秒に設定される。（署名実行者の元の署名の１つが署名エンベロープ１０に採取されながら再提示され、その時間が２．１秒かかった場合、報知は失敗してしまう）。

ソフトウェアオブジェクト

上述の如く、本発明の代表的実施例はオブジェクト指向のプログラミングテクニックを用いて実現されている。また、以下に列挙するのは、本発明を実現する上で用いられる代表的なオブジェクトである。

4.1　署名エンベロープ・オブジェクト。

これは署名行為を保護するために用いられるとともに、内部的に以下のサブオブジェクトを用いている。

4.1.1 署名イメージを表すオブジェクト。このオブジェクトは、イメージデータと、該イメージデータを移入および移出すると共にビ

ットマップ形態で表示またはディスプレイ装置上にダイナミックに表示する方法とを含むものである。

4.1.2 署名の語句的内容では無く、署名の行為自体を表すオブジェクト。このオブジェクトは、個々のペンストロークに関する署名の計測値（筆寸）および付随データを含んでいる。このオブジェクトの主要目的は、照合機能により用いられる計測値を表すことである。このオブジェクトはまた、署名採取時に用いられて生のペンデータを記憶するテンポラリ・オブジェクト（Temporary Object）にも関連し得る。

4.1.3 生のペンデータを表すと共に、このデータに対して例えばストローク数、点の数などの基本的な分析を加えるオブジェクトであって、4.1.2のオブジェクトが計測値を作成し得るように生のペンデータへのアクセスを与えるオブジェクト。

4.2　署名テンプレート・オブジェクト

このオブジェクトは、署名エンベロープ・オブジェクト１０内の計測値の平均値およびこれらの計測値の標準偏差を含んでいる。このオブジェクトは２つの主要機能を有している。即ち、一連の署名エンベロープから“学習”または“登録”する機能と、登録後に署名エンベロープ１０と比較するという機能であり、これは実際には照合機能そのものである。それは、最も直近に署名がなされたエンベロープの作成データおよび作成時刻を除き、いずれの署名エンベロープ１０に関して何も保存しない。この情報はクライアント・アプリケーション２から読み出すことができ、したがって、クライアント・アプリケーションは順番外のエンベロープが照合されているか否かを決定することができる。

4.3　テンプレート・データベース・オブジェクト

このオブジェクトは基本的に、署名者のＩＤに関するテンプレートをコード号化して記憶するに適した手段をクライアント・アプリケーション２に対して与え

るために存在している。

該オブジェクトは２つの主要なサブオブジェクトを含み、それは次のものである：4.3.1 人物に関する基本的情報を保持するとともに、該当人物を参照するアプリケーションにこの情報を交差結合するオブジェクト。該オブジェクトは、アプリケーションデータベースと人物データベースとを２つの結合データベースとともに保持することにより、その機能を達成している。一方の結合データベースは、アプリケーションの各々を該アプリケーションが参照する必要のある人物の全てに対して結合し（この結合データベースは、人物特定時に該当人物に対してアプリケーション自体が使用する特有のＩＤをも含んでいる）、他方の結合データベースは、該当人物を参照するアプリケーションの全てを人物の各々に対して結合している。

したがって、このオブジェクトの主要目的は、ひとりの人物が、多数のアプリケーションの夫々の目的に最も適した手法でこれらのアプリケーションから参照され得る様にすることである。

4.3.2 人物ごとの固有な識別子によりインデックスを付したデータベース内に実際のテンプレートを保持するオブジェクト。

以上のデータベースオブジェクトは両者ともに、特定のタスクに最も適切なファイルの形式および構造を管理する従属オブジェクトを使用している。例えば、複数の項目列を含む、インデックス付きファイル、シーケンシャルファイルおよび結合リストファイルがある。

尚、本発明のアーキテクチャは、署名以外の生体情報を採取かつ照合するためにも活用し得る。例えば、本発明のアーキテクチャは、指紋情報、眼球パターン情報、および声紋情報を含むエンベロープを作成かつ照合する為にも使用され得る。

例

上述した如く、本発明の代表的実施例における署名採取モジュール４は、署名された文書の検査合計値を作成することができる。この文書検査合計は、署名したものと主張された文書がその署名文書であり、さらに、この文書には何らの変

更も加えられていないことを後日に照合すべく使用されるものである。上記の代表的実施例においては、文書の検査合計はオリジナル文書全体を記述するものでなく、したがって、文書の検査合計値からオリジナル文書を引出すことはできない。また、文書検査合計は文書と数理的な関係を有することから、もし文書に変更が加えられれば検査合計値とは数学的に一致しなくなる。本発明のこの特徴は、署名綴じと称されるものである。以下には、本発明に係る署名綴じの特徴の操作例が示されている。

先ず、以下のサンプル文書が与えられたとする：

“私はボルネオに生まれたことをうれしく思う（I am glad I was born in Borneo.〈CR〉〈LF〉”

これは次のＡＳＣＩＩデータに等しい：

49 20 61 6D 20 67 6C 61 64 20 49 20 77 61 73
20 62 6F 72 6E 20 69 6E 20 42 6F 72 6E 65 6F
2E 0D 0A

検査合計値はメッセージ圧縮アルゴリズム（例えば、RSA(RSA Security Inc.)により開発されたＭＤ４またはＭＤ５アルゴリズム）

を用いて作成され、例えば次のような（１６進の）文書検査合計が作成される：

89F32145AB321AF7C411FB76543F0CFC。

ここで、署名エンベロープは次の情報を含んでいる：

・バージョン番号（整数）
・機器のシリアル番号（整数）
・機器のブート時刻（整数）
・機器とオペレーティングシステムの種類（整数）
・署名者が主張するＩＤ（可変長、キャラクタ）
・重要プロンプト（可変長、キャラクタ）
・署名筆寸の列（整数）
・署名の日付／時刻（整数）

・署名イメージ（可変長）

・ファイル検査合計（キャラクタ）

・エンベロープ検査合計（キャラクタ）

コード化されたデータ・ブロックに移出されるときに、これらの情報には次の長さ情報が加えられる：

・エンベロープの合計長（整数）

・署名者が主張するＩＤの長さ（整数）

・重要事項の長さ（整数）

・署名イメージの長さ（整数、但し、署名がなければゼロ）

上記署名イメージは詳細には次の様にして記憶される：

・開始座標値

・前の座標値と次の座標値との間の差の列

また、これらのデータ項目の各々は、次のようにして構成される。

もし次のキャラクタを整数として見た場合に負であれば、そのキャラクタの残りのビットは次の条件を表すためのフラグとして用い

られる。

・ストロークエンド（End of Stroke）

・次の値は２キャラクタ長であること

・１つおいた次の値は２キャラクタ長であること

・次の値は符号を変えていること（負から正へ、またはその逆）

・１つおいた次の値は符号を変えていること

・次の値は反復計数値（Repeat Count）（常に正）であること

例えば、署名が幾何学的に鋭角的な文字“Ｖ”で始まるとすれば、そのイメージは次のように表される：

１．Ｙ座標値が２０であることを示す、正のキャラクタ

２．Ｘ座標値が０であることを示す、ゼロキャラクタ

３．反復回数を表すビットがセットされた、負のキャラクタ

４．１０の値を有するキャラクタ

５．Ｙが負に変わることを表すビットがセットされた、負のキャラクタ

６．Ｙの差が２（即ち－２）であることを示す、正のキャラクタ

７．Ｘの差が１であることを示す、正のキャラクタ

８．反復回数を表すビットがセットされた、負のキャラクタ

９．１０の値を有するキャラクタ

１０．Ｙが正に変わることを表すビットがセットされた、負のキャラクタ

１１．Ｙの差が２である（ここでは＋２）キャラクタ

１２．Ｘの差が１であるキャラクタ

１３．ストロークエンドであることを表すビットがセットされ

た、負のキャラクタ。

ここで、クライアント・アプリケーションが、署名を採取して上記のボルネオ（Borneo）文書にこの署名を付加することを企図したとする。ＯＳ／２オペレーティングシステムでは、以下の情報が用意される。

－署名採取ウインドウ２０が挿入されるウインドウ（例えば図３Ａの３０）に対するＯＳ／２の識別子、

－署名者を特定する、ゼロキャラクタで終わるキャラクタ列、

－重要事項を与える、ゼロキャラクタで終わるキャラクタ列、

－署名イメージの採取が望まれるのであれば、ゼロ以外の値を有する整数、

－完全性検査合計のためのシークレット・アプリケーションキーを与えるキャラクタ列、

－このシークレットキーの長さを与える整数、および

－検査合計が行われるべき文書を記憶するファイルの名前を与える、ゼロキャラクタで終わるキャラクタ列。

署名採取コンポーネントは次に、適切な重要事項２２と、署名者が主張したＩＤとを伴う署名採取ウインドウ２０を表示する。このコンポーネントは指定されたファイルを縦覧して検査合計値をも作成する。この署名採取ウインドウ２０上でユーザーがペンを走らせる間、ペンデータは、ＸおよびＹの移動値および時間差の形態で内部的に記憶される。もしユーザーが引続いて“ＯＫ”制御部２８を

起動すれば、これらの移動値は絶対距離を表すべく縮尺が付けられ、さらに、署名の計測値を求めるべく分析される。最終的に、署名イメージが要求されれば、上記ペンデータはイメージ列に変換される

（タイミング情報の全ては取り除かれる）。

この時点で、クライアント・アプリケーション２には、数字コードにより相互作用の結果が通知される。

０．エンベロープの作成に成功

１．署名は放棄されたー即ち、ユーザーが“取消し”制御部を起動した

３．無効な（例えば長さがゼロの）ＩＤを主張した

４．無効な（例えば長さがゼロの）重要プロンプト

５．検査合計が行われるべきであったファイルの誤った読み込み

【図１】

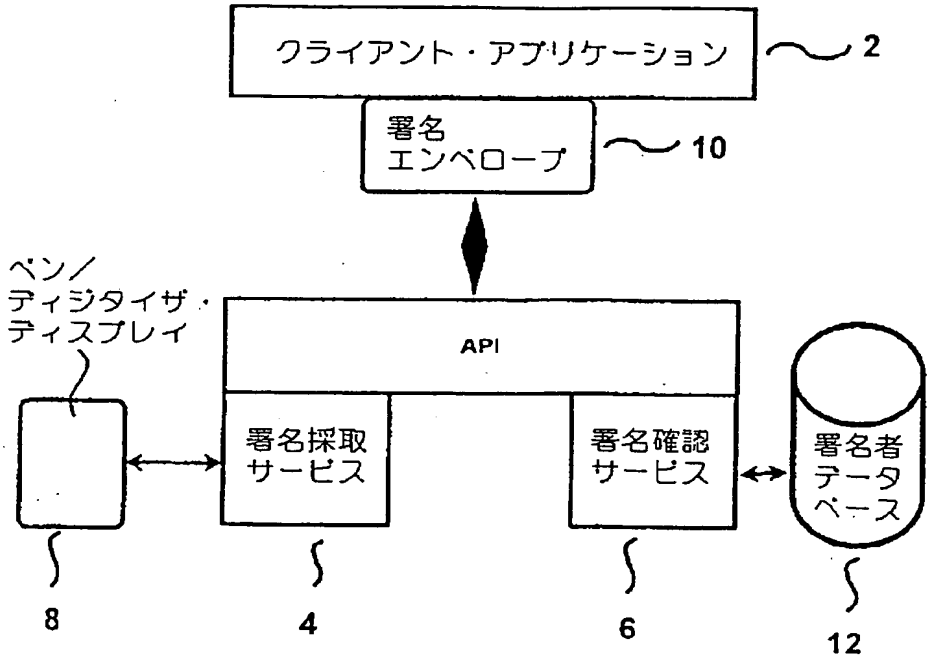
クライアント・アプリケーション
2
署名
エンベロープ
10
ペン／
ディジタイザ・
ディスプレイ
API
署名採取
サービス
署名確認
サービス
署名者
データ
ベース
8
4
6
12

FIG. 1

【図２】

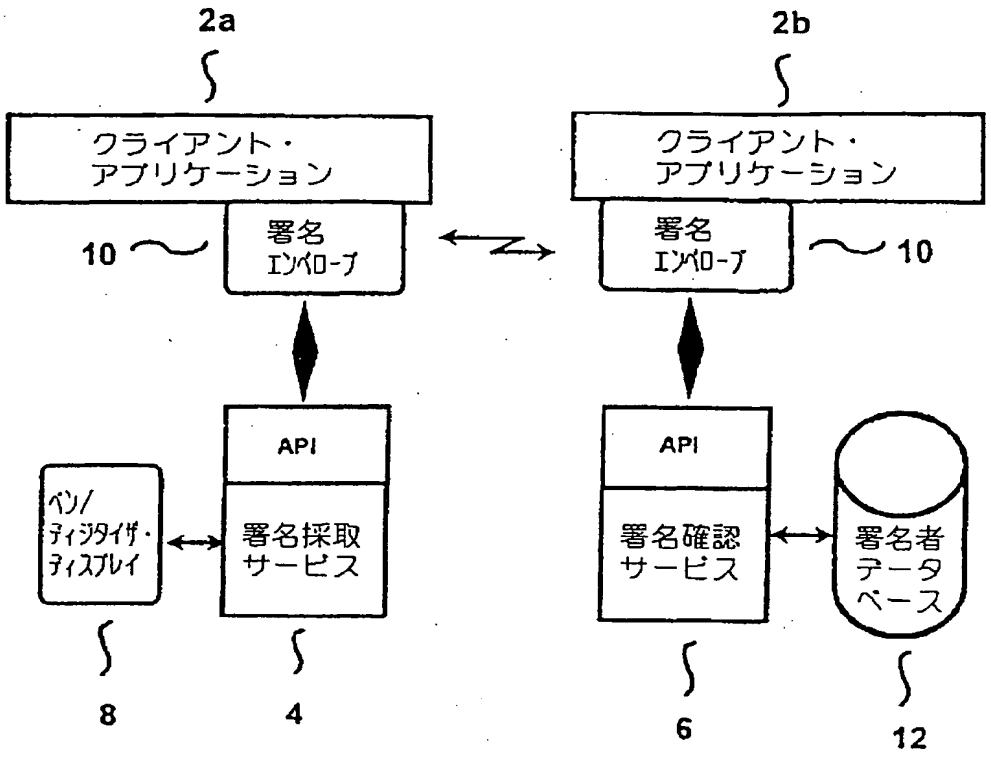
2a
2b
クライアント・
アプリケーション
クライアント・
アプリケーション
署名
エンベロープ
署名
エンベロープ
10
10
API
API
ペン/
ティジタイザ・
ディスプレイ
署名採取
サービス
署名確認
サービス
署名者
データ
ベース
8
4
6
12

FIG. 2

【図３】

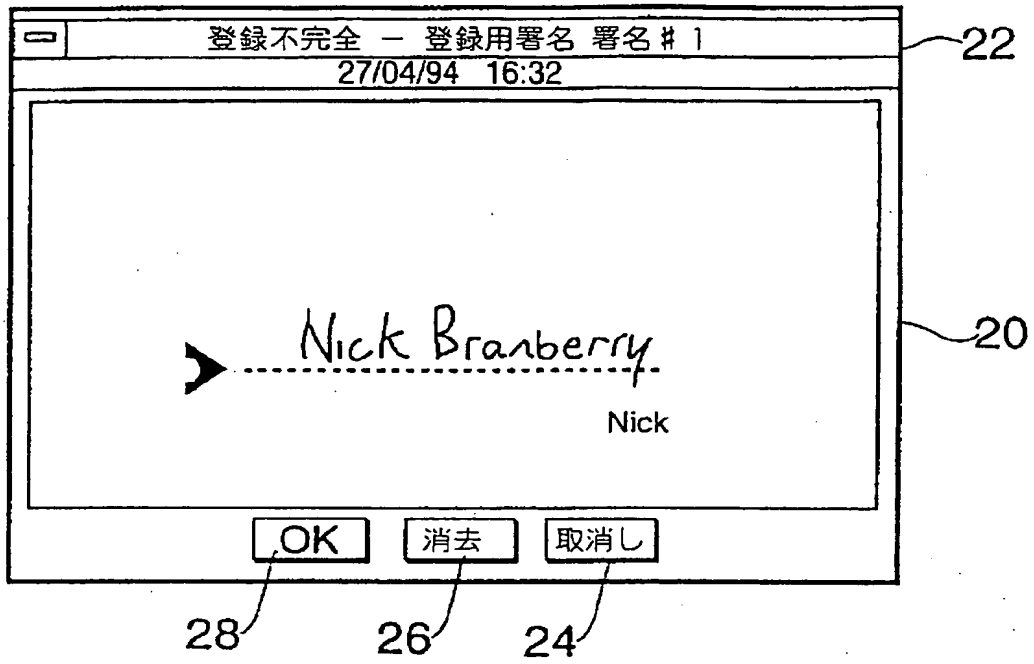
登録不完全 － 登録用署名 署名＃１
27/04/94 16:32
22
Nick Branberry
Nick
20
OK
消去
取消し
28
26
24

FIG. 3

【図３】

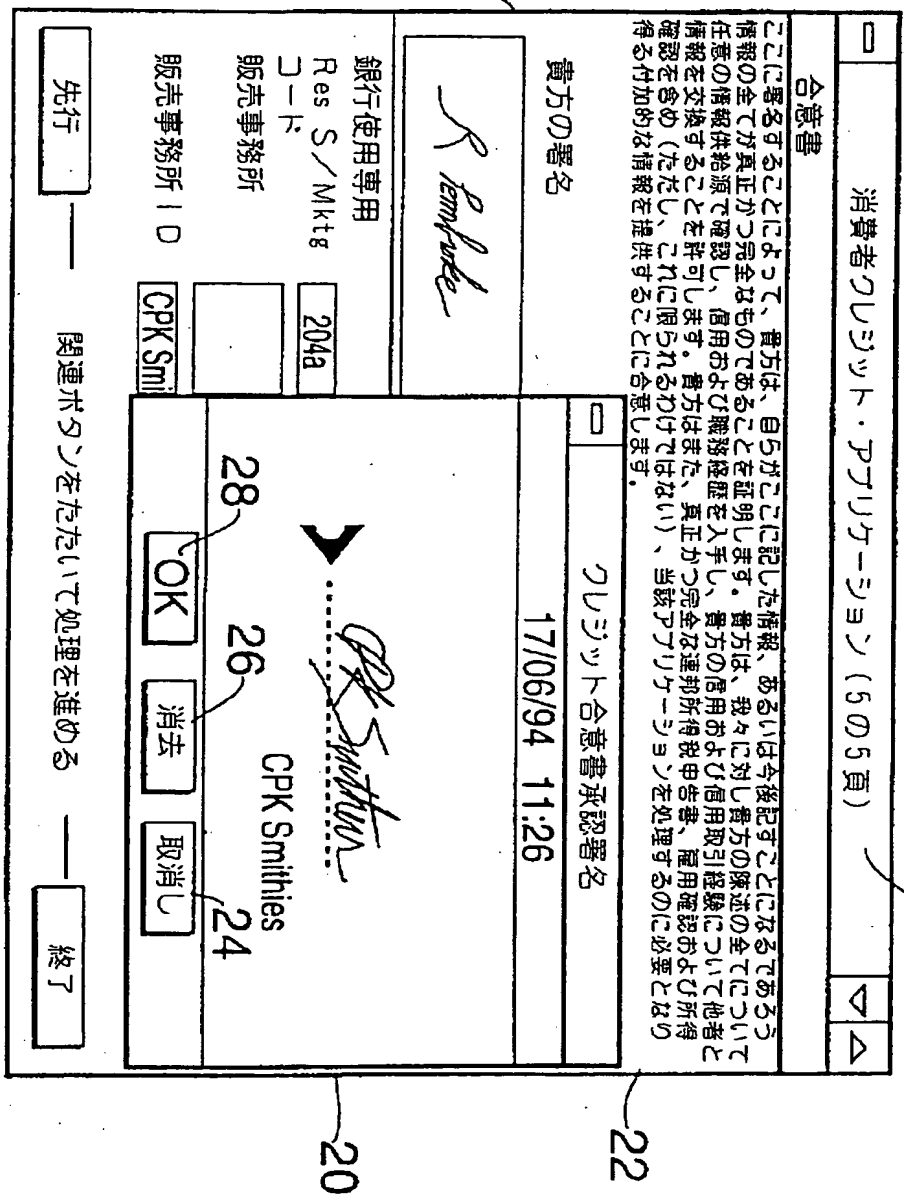
消費者クレジット・アプリケーション（５の５頁）
32
合意書
ここに署名することによって、貴方は、自らがここに記した情報、あるいは今後記すことになるであろう情報の全てが真正かつ完全なものであることを証明します。貴方は、我々に対し貴方の陳述の全てについて任意の情報供給源で確認し、信用および職務経歴を入手し、貴方の信用および信用取引経験について他者と情報を交換することを許可します。貴方はまた、真正かつ完全な連邦所得税申告書、雇用確認および所得確認を含め（ただし、これに限られるわけではない）、当該アプリケーションを処理するのに必要となり得る付加的な情報を提供することに合意します。
貴方の署名
30
R Template
クレジット合意書承認署名
17/06/94 11:26
22
銀行使用専用
Res S／Mktg コード
204a
販売事務所
販売事務所ＩＤ
CPK Smi
CPK Smithies
28
OK
26
消去
24
取消し
20
先行
関連ボタンをたたいて処理を進める
終了

FIG. 3A

【図４】

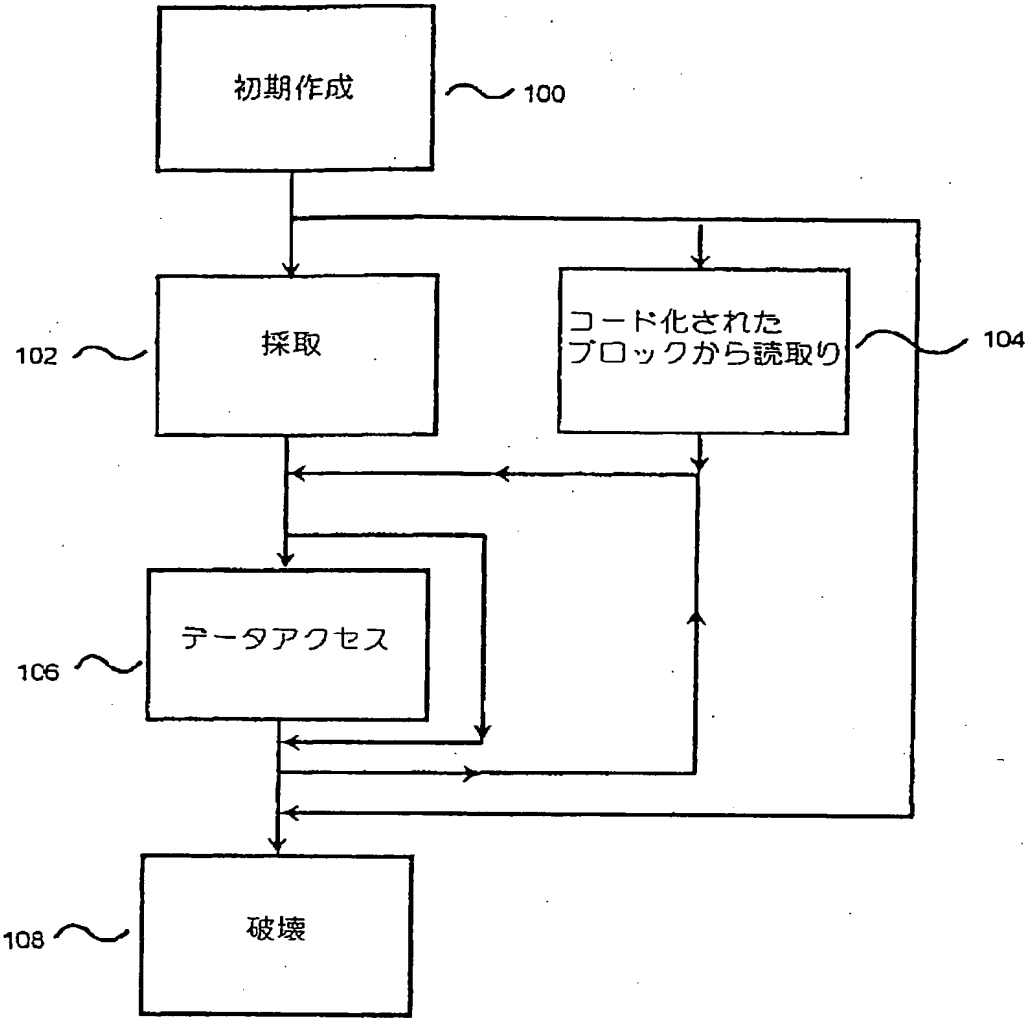

FIG. 4

【図５】

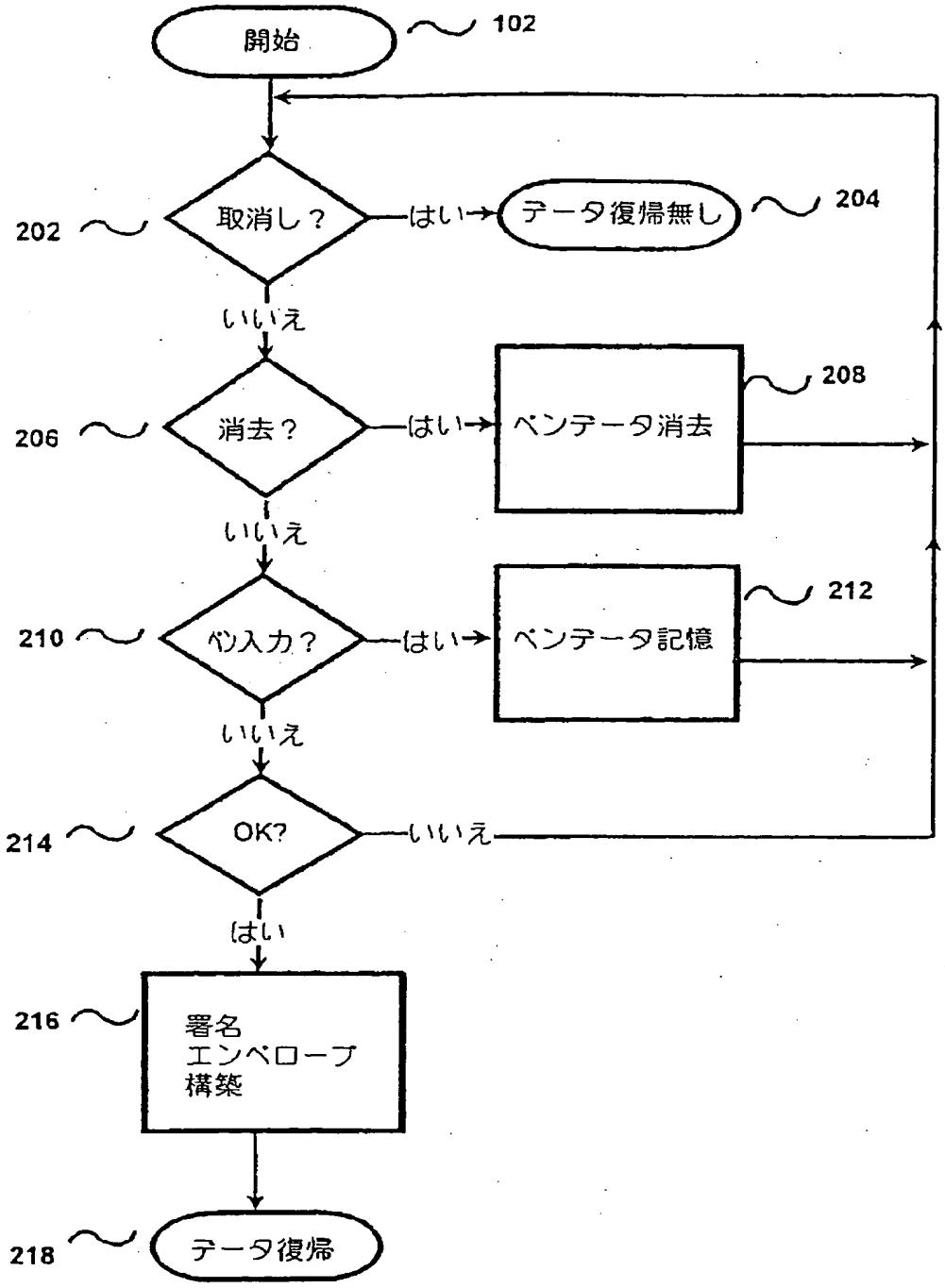
開始
102
取消し？
はい
データ復帰無し
204
202
いいえ
消去？
はい
ペンデータ消去
208
206
いいえ
ペン入力？
はい
ペンデータ記憶
212
210
いいえ
OK?
いいえ
214
はい
署名
エンベロープ
構築
216
データ復帰
218

FIG. 5

【図６】

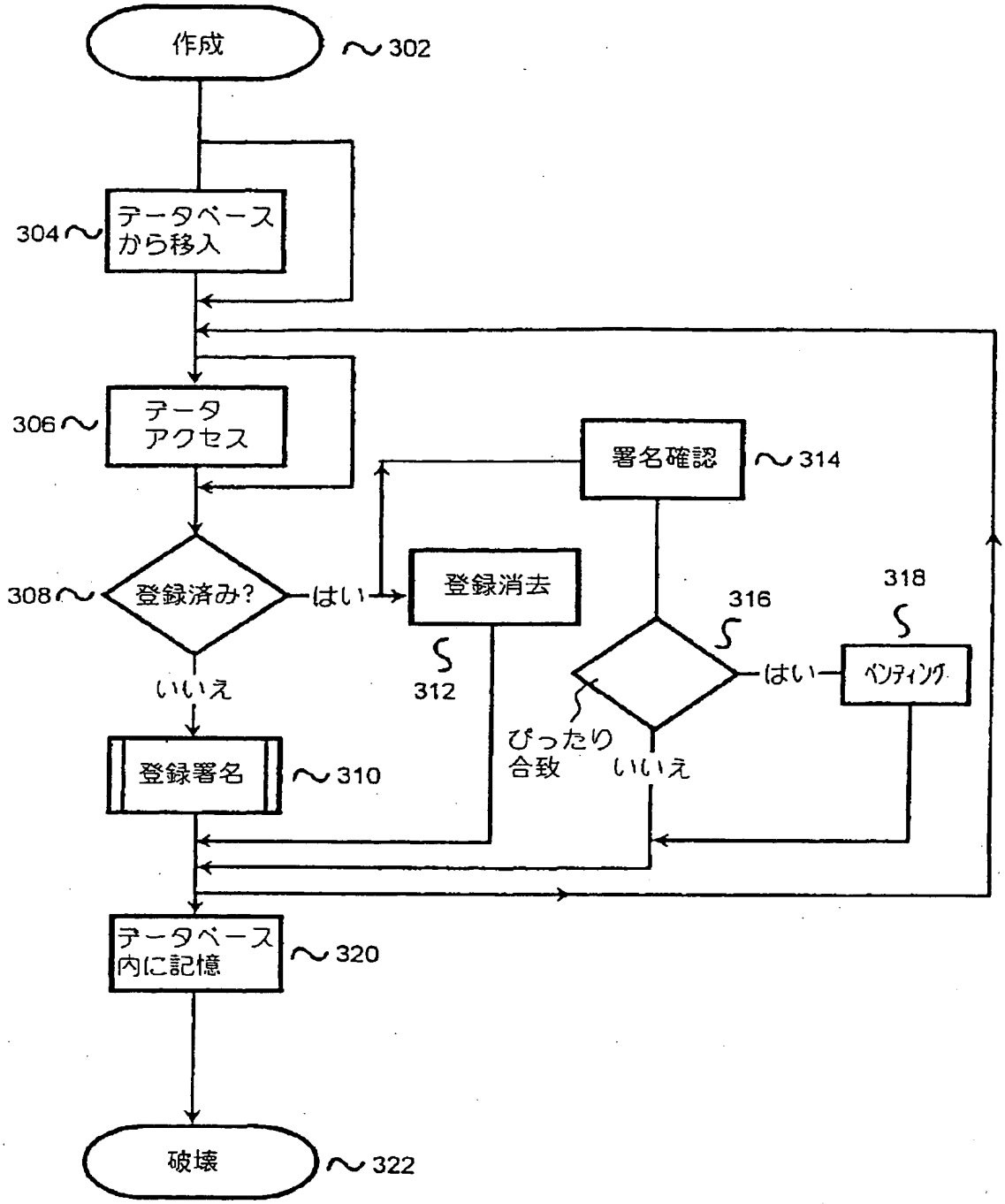
作成
302
304
データベースから移入
306
データアクセス
署名確認
314
308
登録済み?
はい
登録消去
312
316
318
ペンティング
はい
いいえ
ぴったり合致
いいえ
登録署名
310
データベース内に記憶
320
破壊
322

Fig. 6

【図7】

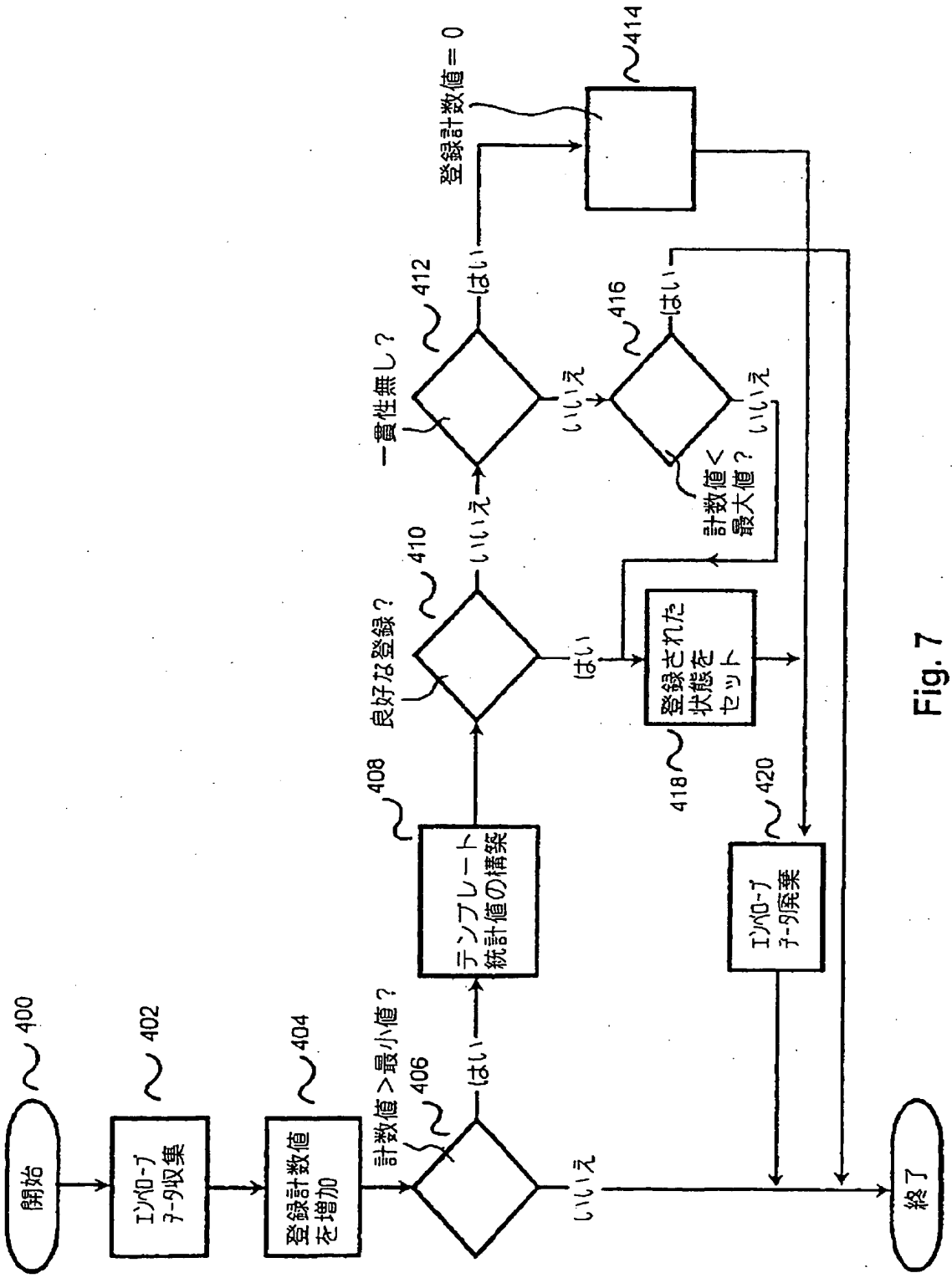
開始
400
エンロール データ収集
402
登録計数値を増加
404
計数値 > 最小値 ?
406
はい
いいえ
テンプレート 統計値の構築
408
良好な登録 ?
410
はい
いいえ
一貫性無し ?
412
はい
いいえ
登録計数値 = 0
414
計数値 < 最大値 ?
416
はい
いいえ
登録された状態をセット
418
エンロール データ廃棄
420
終了

Fig. 7

【図８】

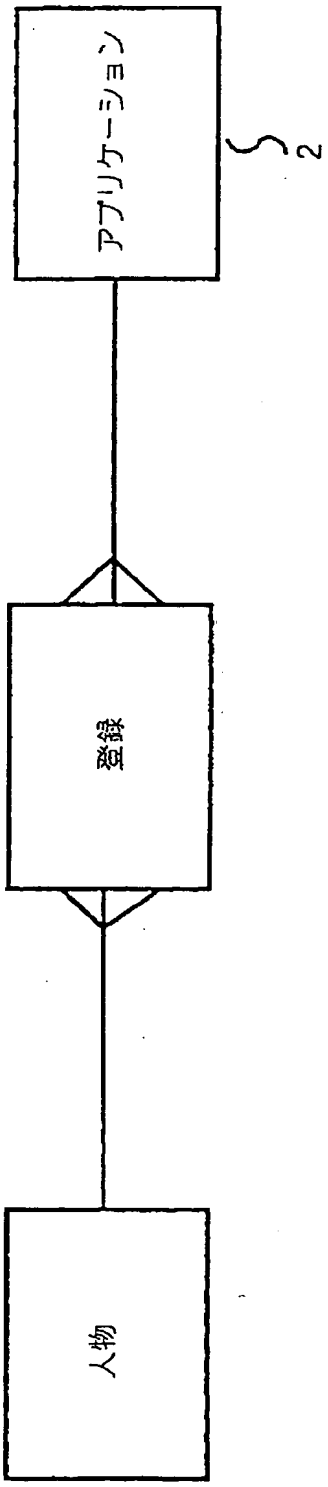

Fig. 8

【図９】

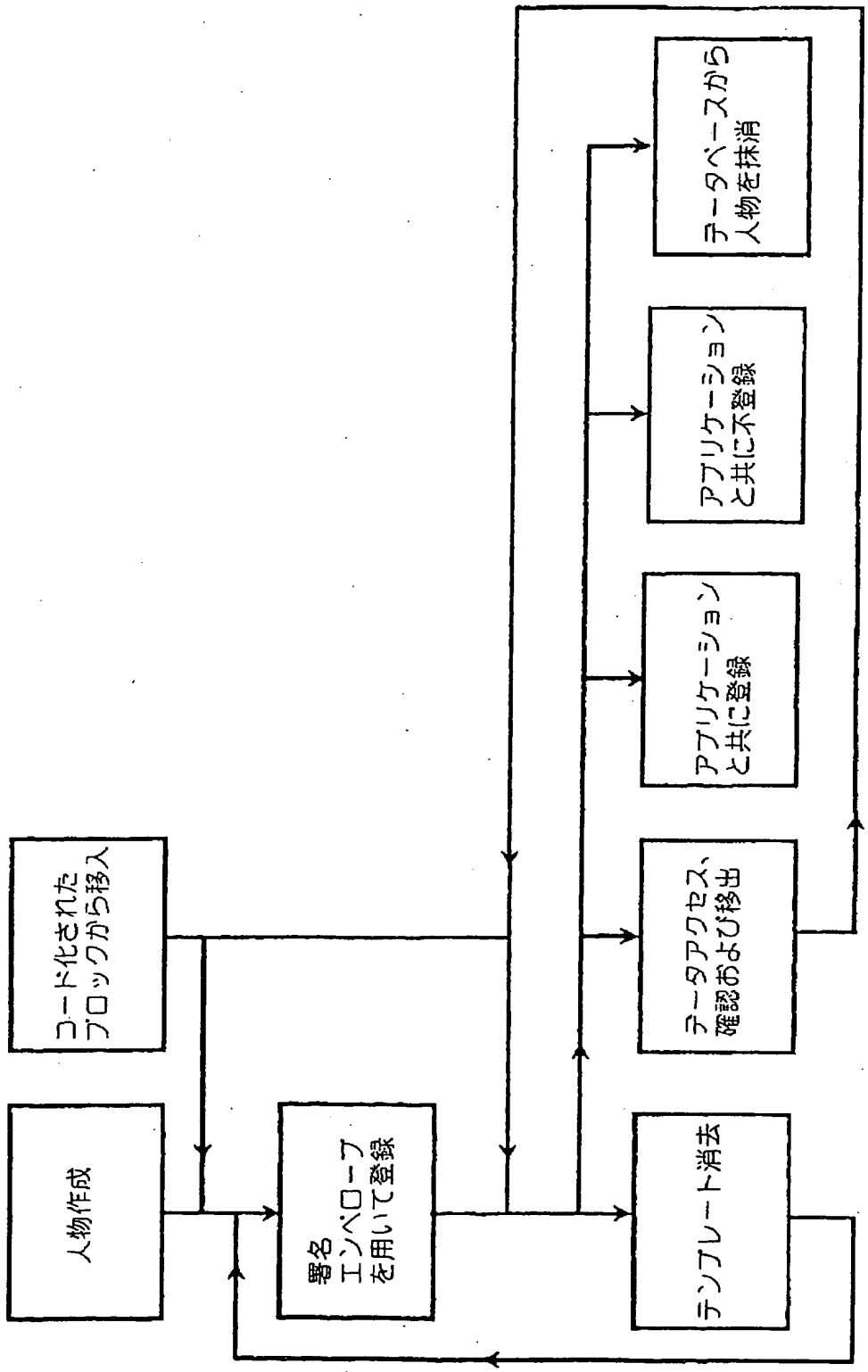
人物作成
コード化されたブロックから移入
署名エンベロープを用いて登録
テンプレート消去
データアクセス、確認および移出
アプリケーションと共に登録
アプリケーションと共に不登録
データベースから人物を抹消

Fig. 9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/11016

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :Please See Extra Sheet.
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : Please See Extra Sheet.

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US, A, 5,195,133 (KAPP ET AL.) 16 March 1993, see Figure 5, column 2, lines 22-42, column 3, line 61 through column 4, line 12 and column 5, line 53 through column 6, line 68.	1-2, 7-17, 38-41, 46-52, 57-73 --- 3-6, 42-45, 53-56
X --- Y	US, A, 5,297,202 (KAPP ET AL.) 22 March 1994, see column 5, line 53 through column 7, line 3.	1-2, 7-17, 38-41, 46-52, 57-73 --- 3-6, 42-45, 53-56
Y	US, A, 5,322,978 (PROTHEROE ET AL.) 21 June 1994, see Figure 6.	1-17, 38-73

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be part of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
04 OCTOBER 1995	31 OCT 1995
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer ANDREW W. JOHNS Telephone No. (703) 305-8576

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/11016

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,495,644 (PARKS ET AL.) 22 January 1985, see Table 1 in columns 13-16.	3-6, 42-45, 53-56
A	US, A, 5,091,975 (BERGER ET AL.) 25 February 1992.	1-73
A	US, A, 5,339,361 (SCHWALM ET AL.) 16 August 1994.	1-73
A	Newsbytes News Network, 8 March 1993, "Mobile World--Signing Documents Remotely By Pen Computer."	1-73
A	Computerworld, 14 June 1993, page 57, "Execs Can Sign Papers By Remote Control; Pen Computing-Based System Allows Addition of Handwritten Notes."	1-73

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/11016

A. CLASSIFICATION OF SUBJECT MATTER:
IPC (6):

G06K 9/00

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

382/119, 232

B. FIELDS SEARCHED
Minimum documentation searched
Classification System: U.S.

382/119, 120, 121, 122, 123, 232; 178/18; 340/825.3, 825.33, 825.34; 283/70, 75; 395/155, 161; 380/23

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, MW, SD, SZ, UG), AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TT, UA, UG, UZ, VN

(72)発明者 ニューマン, ジェレミー マーク
イギリス国, サマセット ビーエー11 1イーエル, フロム, シェパーズ バルトン 11

【要約の続き】
評点を得るための署名エンベロープ内に記憶された一揃いの計測値と比較される。本発明は、文書の性質、重大さ及び／又は内容に関して署名者に警告するための重要プロンプト機能を含んでいる。重要プロンプト（22）は同様に署名記録の一部として署名エンベロープの中に記憶することができる。